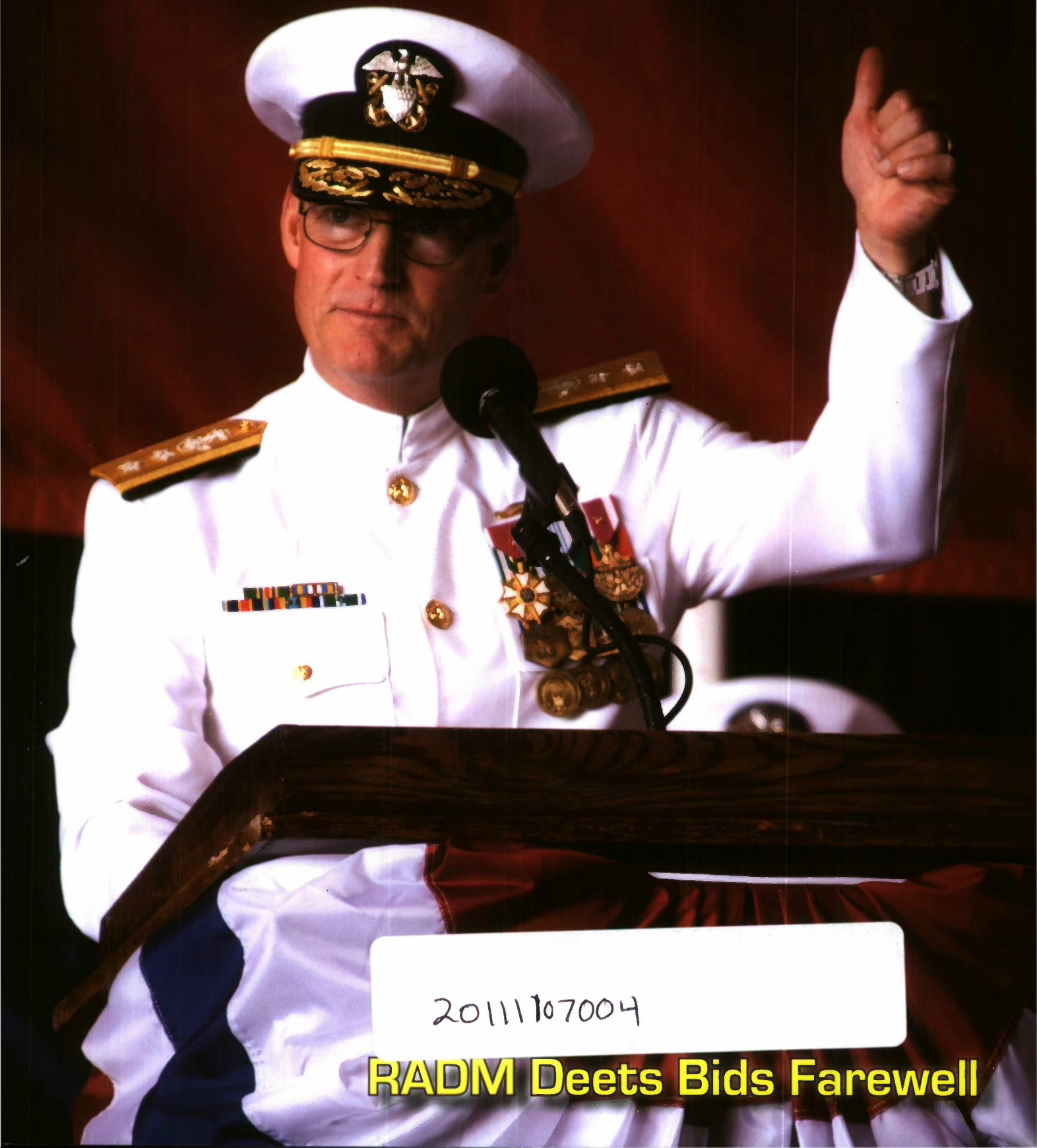
InfoDOMAIN

DECISION SUPERIORITY FOR THE WARFIGHTER

FALL 2011



RADM Deets Bids Farewell

InfoDOMAIN

DECISION SUPERIORITY FOR THE WARFIGHTER

FEATURES

DEPARTMENTS

FRONT COVER: *RADM Edward H. Deets III, NETWARCOM Commander, gives a "thumbs up" on the Navy and his accomplishments over the past 32 years. For more information about Deets' retirement ceremony see pages 26-27. (Photo by Robin D. Hicks)*

Commander, Navy Cyber Forces
RDML Gretchen S. Herbert

Deputy Commander
Mr. F. Scott DiLisio

Public Affairs Officer
Ms. Darlene Goodwin

Deputy PAO / Editor
Mr. George D. Bieber

Associate Editor
MC1(SW) Joshua J. Wahl

Visual Information Specialist
Mr. Robin D. Hicks

Production
McDonald & Eudy Printers, Inc.
Temple Hills, MD

InfoDOMAIN is the professional magazine of Navy Cyber Forces that promotes the advancement of Information Dominance through an open exchange of better practices, tactics, and current and future strategies to meet the global challenges of the information domain.

Information contained in ***InfoDOMAIN*** does not necessarily reflect the official views of the U.S. Government, the Department of Defense or the Department of the Navy. Editorial content is prepared by the Public Affairs Office of Navy Cyber Forces.

Articles for publication in ***InfoDOMAIN*** should be submitted through the appropriate command representative. Security and policy review must be completed by submitting commands before articles can be considered for publication. Address all correspondence to Editor, InfoDOMAIN, Navy Cyber Forces, Public Affairs Office, Joint Expeditionary Base Little Creek - Fort Story, 2465 Guadalcanal Road, Suite 10, Virginia Beach, VA, 23459-3243; telephone (757) 417-7958 ext. 5, DSN 537-7958 ext. 5, FAX (757) 492-8702. Comments or queries may also be forwarded to: george.bieber@navy.mil

Photo by MC1(SW) Joshua J. Wahl

RDML Gretchen S. Herbert, CYBERFOR Commander

RDML Gretchen S. Herbert, an Information Professional (IP) officer, took command of Navy Cyber Forces in June 2011 (see Change of Command story, page 25). In her first interview with InfoDOMAIN magazine, Herbert provides insight into her Navy career and her priorities as leader of the Navy's global Type Command (TYCOM) for C5I (Command, Control, Communications, Computers, Combat Systems and Intelligence).

. . . continued on Page 4

InfoDOMAIN: Could you please tell our readers about your Navy career, and specifically how your previous assignments have prepared you for your current position.

RDML Herbert: When I joined the Navy in 1984, the term "cyberspace" wasn't heard much ... if it even was mentioned at all! Military strategy between bipolar powers was focused on nuclear deterrence – the Soviet Union and the spread of communism was our greatest national security threat. While certainly a challenging time, the Cold War was in many respects, much "simpler." We knew and understood our enemy; we knew their capabilities and largely, their intent.

Today threats aren't so clear cut, especially in the cyber and information domains. Cybersecurity and computer network operations are relatively new missions that were not on people's radar 25 years ago. Today however, many – if not most – of our military operations depend on unfettered access to cyberspace. Cyberspace has clearly changed the way we interact as a Navy, as a military, and as a global community.

Throughout my career, I've had the opportunity to work in many different "specialty" areas that helped build the skills and competencies that contribute to the Information Dominance vision. When I began my Navy service in the Sound Surveillance System (SOSUS), tracking Soviet submarines, it had a very operationally focused and I&W (Indication and Warning) cueing element to the mission. In the years that followed, I had the opportunity to broaden my experience in assignments related to the information domain, including satellite communications, Naval computer and telecommunications, HF (High Frequency) over the horizon radar operations, and as an instructor at the Joint Forces Staff College, where I taught Joint Command, Control, Communications, Computer and Intelligence courses.

"Small scale technologies, wielded by a malicious actor or a 'nuisance hacker' can have a far-reaching, detrimental impact. Literally, with a few key strokes one can disable a capability anywhere in the world."

Additionally, afloat assignments as a Combat Systems Officer and the Strike Group N6 (assistant Chief of Staff for Communications and Information Systems) provided me with a myriad of opportunities to learn more about the capabilities, challenges and future requirements for C5I Fleet operations and readiness. And finally, while serving on the OPNAV (Chief of Naval Operations) staff, I learned a great deal about resource requirements, the budget process, and the efforts and challenges with transitioning concepts and new technologies into real, tangible capabilities and interoperable systems delivered to the Fleet.

So while nuclear deterrence was a predominant focus when I joined the Navy in 1984, today, deterrence can be partially achieved through the development and training of a highly skilled cadre of cyber professionals – and the Information Dominance Corps is central to that effort.

For the Department of Defense and the Navy to operate freely within the cyber domain, we must devote sufficient resources and personnel to ensure mission success. That's why I'm so thrilled to be associated with the talented and dedicated men and women of Navy Cyber Forces. We are in the right place at the right time for making significant and consequential improvements to the way we prepare and deliver cyber forces and capabilities to our Navy. It truly is an exciting time to be a part of this important Type Command.

InfoDOMAIN: What are your current focus areas?

RDML Herbert: The Navy Cyber Forces team is collectively advancing Fleet C5I readiness throughout the domain, but the areas that I have been particularly focused on in the past few months include four areas.

Building Electronic Warfare Proficiency

The Fleet Electronic Warfare Center (FEWC) is aggressively pursuing improved EW readiness from five lines of operation – mission accountability, building EW skills and expertise for our enlisted, our officer corps, material (equipment) modernization to pace the threat, and building a robust and relevant Fleet EW training. Some of the specific efforts include establishing EW as a Primary Mission Area, establishing EW in DRRS-N (Defense Readiness Reporting System – Navy), formalized Tactics Seminars, performing Technical Assist Visits for Surface Unit training, and establishing training Electronic Warfare Officer Training continuums. These are just a few of the things currently in work designed to dive into the weeds and specifically pinpoint detailed areas for improvement. Moreover, these initiatives address an overarching strategy to reverse the decline in EW readiness and the atrophy of EW proficiency – throughout the tactical, operational and strategic spectrum of operations.

Fixing, Consolidating and Reducing the Number of Afloat Applications

As our systems, processes and procedures became more technically complex, the number of associated software applications have proliferated throughout the Fleet. In some cases, new software applications have resulted in improved performance, reduction in manual operations, and added capabilities. Unfortunately in other cases, applications that were designed for a stable, high bandwidth, low latency networking environment do not perform optimally in an afloat environment.

That shouldn't be a great revelation to any of us, and yet, the number of software apps that continue to be installed on our afloat networks are taking a toll ... in network performance, system supportability, and as burden to the operator and the system administrator. Navy Cyber Forces has been spearheading a comprehensive effort with Fleet, TYCOM, SYSCOM (Systems Commanders) and Resource Sponsor stakeholders to thoroughly review the performance of software applications – with the goal of fixing those that are broken or removing them from our afloat networks. Additionally, the Fleet FAM (Functional Area

. . . continued on Page 6

AT A **GLANCE**

RDML Gretchen S. Herbert is a native of Rochester, NY. She graduated from the University of Rochester in 1984, receiving her commission through the Naval ROTC program. She holds a Masters degree in Systems Technology (Space Systems Operations) from the Naval Postgraduate School and a Masters degree in Military Studies from the Marine Corps Command and Staff College.

During her early assignments, Herbert served within the Integrated Undersea Surveillance System at Naval Facility Bermuda; at Commander, Oceanographic Systems Atlantic; and at Naval Ocean Processing Facility, Dam Neck, Virginia Beach, VA.

Additional shore assignments include satellite communications officer at Headquarters, U.S. Naval Forces Europe; executive officer, Fleet Surveillance Support Command; Joint Command, Control, Communications, Computer and Intelligence instructor at the Joint Forces Staff College; commanding officer, Naval Computer and Telecommunications Station Washington; branch head, Naval Networks for OPNAV N6; and assistant Chief of Naval Operations for the Next Generation Enterprise Network.

She also served as director of the Communications, Networks and Chief Information Officer (CIO) Division on the staff of the Deputy Chief of Naval Operations for Information Dominance (OPNAV N2/N6).

Fleet assignments include combat systems officer embarked in USS George Washington (CVN 73) where she deployed to the Arabian Gulf in support of Operations Southern Watch, Enduring Freedom and Iraqi Freedom; and assistant chief of staff for Communications and Information Systems (N6) to commander, Carrier Strike Group 7 embarked in USS Ronald Reagan (CVN 76) where she deployed to the Western Pacific and Arabian Gulf with Ronald Reagan Strike Group.

In June, 2011, Herbert assumed command of Navy Cyber Forces at Joint Expeditionary Base Little Creek-Fort Story, Virginia Beach, VA.

FORCE CHAPLAIN'S THOUGHTS

I recently attended my faith group's annual conference in Cincinnati. While I was manning the Chaplain Endorsement Agency booth, an older woman approached me saying, "You're the guy. You're the chaplain."

After a few hints I made the connection. I had been invited to speak in chapel at my seminar on Veterans Day almost 11 years earlier. I was given a room at a dorm where this woman and her husband were serving as dorm parents. The husband was a World War II veteran.

As we talked they explained they were in the process of reviewing his Army records to make sure everything was in order. They had found several mistakes, some of which affected his benefits, some of which were simply unfortunate.

He showed me a pair of glider wings and explained he had been part of a short-lived program that used a glider type apparatus instead of a parachute for airborne assaults. The Army found the mortality rate for these servicemen to be about 65 percent and scrapped the program after the war.

This man had been part of the D-Day invasion using a glider and survived. He explained that they had been required to go to jump school with the paratroopers, but they were in such a rush to get them on to glider training and ready for the invasion that they weren't allowed to attend the graduation ceremony. They never received their jump wings.

Although he understood, he had always regretted not receiving a pair of jump wings. He was unaware I had just graduated from jump school and had picked up an extra pair of wings. I found out a couple of staff members at the seminary were Airborne. We devised a plan to present a pair of jump wings to him the next morning at chapel.

We allowed his wife to pin the jump wings next to his glider wings. The students and staff caught the spirit of the occasion and gave him a long standing ovation, complete with cheers as if it were a great sports event.

The wife told me her husband had died recently, but both had reflected often on that chapel service and the encouragement they both received from it.

This Veterans Day please take the time to thank a Veteran, young or old, for their sacrificial service to their country. A little encouragement or a small act of kindness can go a long way in fulfilling the spirit of Veterans Day.

Chaplain Mac

My Domain continued...

Management) team is validating that any applications currently installed, or to be fielded, meet the criteria for long term sustainability (i.e. they are funded for training, upgrades and logistic support), interoperability, and accreditation and authority to operate on Navy networks.

As we continue this process, we are soliciting feedback directly from the Fleet, to validate that fixes are successful, training is adequate and that problematic applications are removed from the network. The team is making great progress, but this effort is a marathon, not a sprint. With over 900 different application versions or imbedded apps residing on our networks, there are plenty of opportunities for improvements!

Development of the Cyber Workforce

Navy Cyber Forces is committed to recruiting, developing and retaining a highly skilled and professional cyber workforce. To that end, we are continuing our engagement with OPNAV N2/N6 (Deputy CNO for Information Dominance), Fleet Cyber Command, 10th Fleet, OPNAV N1 (Manpower), and the Navy's entire Manpower, Personnel, Training and Education (MPT&E) organization to deliver a top notch, highly trained and effective workforce to counter the worldwide cyber threat. To be effective and efficient our workforce must consist of the right mix of military (including officer, enlisted and reserves) as well as civilian members with the right skill sets to ensure our freedom of maneuver in the information domain and to deny our adversaries such freedom when necessary. We are working hard to identify capability gaps within our workforce as well as identify emerging mission areas that demand a cyber workforce fully prepared to meet all cyberspace challenges. The recently revamped "IT of the Future" training for Information Systems Technicians is one example of ways we are addressing shortfalls in historical training and building the workforce of tomorrow. We are also partnering with OPNAV N2/N6 to complete a Navy-wide Zero Based Review to baseline our cyber manpower and to identify gaps.

Training our Fleet

Training our Fleet through the Fleet Readiness Training Plan (FRTP): In our role as the global C5I Type Commander, we are responsible for C5I readiness assessments of Fleet units (afloat – ships, submarines and aircraft carriers, and ashore – Naval Computer and Telecommunications Area Master Stations, Navy Information Operations Commands, Fleet Intelligence Detachments, and Fleet Intelligence Adaptive Force). To ensure that we continue to successfully deliver both current C5I capabilities and future readiness, we are scrutinizing C5I metrics and reports from returning Strike Groups and Independent deployers, participating in Fleet assist and training visits, and certifying units for participation in the integrated phase of training. Additionally, we continue to certify ashore units for sustained operations – 24/7/365. And finally, our readiness team conducts monthly reviews of the units, assessing their DRRS-N inputs, mitigating readiness issues by shifting funding priorities or submitting requests to higher headquarters for resources (manning or funding).

InfoDOMAIN: What makes Cyber warfare so challenging?

RDML Herbert: Cyber warfare is rapidly changing. The internet was originally designed to be a collaborative, open and transparent environment. The rapid flow of information was more important that content integrity, identity authentication, and data protection. But as I said earlier, the Navy and the nation have come to rely on our networks, and on unrestricted access to the electromagnetic spectrum. That access is complicated, however, by the low barriers for entry into cyberspace.

Small scale technologies, wielded by a malicious actor or a "nuisance hacker" can have a far-reaching, detrimental impact. Literally, with a few key strokes one can disable a capability anywhere in the world. As former Director of National Intelligence retired VADM Mike McConnell has said, you can disable power grids which in the heat of summer or the chill of winter could be catastrophic. Combine that with loss of confidence in our financial system – or a Commander's loss of confidence in his or her weapons systems – and the impact is magnified. And when attribution is difficult or time-consuming, deterrence as a strategy in cyberspace is particularly challenging.

Bottom line, the asymmetric impact of an attack in cyberspace can be profound ... and is a very real threat.

InfoDOMAIN: How do you foresee CYBERFOR being more efficient in the face of tightening federal budgets?

RDML Herbert: It is going to be challenging, because over the past several years, we have already looked across the domain to get rid of duplicative capabilities – making sure we don't have overhead in any of the staffs and functions. So, now we are down to the bone in where we might find further efficiencies. We have to look at leveraging existing or comparable talent and expertise across the domain and across other services and industry, to find other opportunities for savings, shared training or incorporating best practices. Additionally, I will continually look at meeting our top priorities, with focus, resources and attention, while identifying those areas which might not receive the same level of effort that they had in the past. In a resource constrained environment, I'll focus our resources and personnel on only those efforts that contribute to Fleet Readiness, and to building and sustaining a premier cyber and information dominance workforce.

InfoDOMAIN: What do you believe will be the most significant impacts of the proposed move of CYBERFOR headquarters to the former Joint Forces Command facility in Suffolk?

RDML Herbert: While the planned move to Suffolk won't impact CYBERFOR's mission, I believe it will enhance our working environment. Since taking command of Navy Cyber Forces, I've been very

impressed by the dedication and professionalism of the entire CYBERFOR workforce. They've been doing world-class work – and are at the top of their game – despite the fact that they haven't been working in "world-class" accommodations! That's all going to change when we execute the move to Suffolk. The former Joint Forces Command spaces are high tech and a significant improvement over the "temporary" facilities that the co-located staffs of Naval Network Warfare Command, Navy Cyber Defense Operations Command and Navy Cyber Forces have occupied over the last decade!

InfoDOMAIN: What is one goal you would like to achieve that, upon your departure, people would say, "I'm glad I served under Admiral Herbert."

RDML Herbert: That's an easy one. I would be pleased to know that the men and women of Navy Cyber Forces felt professionally challenged, knew that their talents were valued and that they were proud of their role in shaping our Navy's future.

Navy-wide Training Management System Moves to New Web Address

By Ed Barker, Naval Education and Training Command Public Affairs

PENSACOLA, FL – As part of network policy and standardization initiatives, a new home page Web address for the Navy's Training Management System was implemented Aug. 6.

The Navy's Corporate enterprise Training Activity Resource System (CeTARS) is the authoritative Student Training Management System for Manpower, Personnel, Training and Education (MPTE) and serves as the data source for all formal Navy training statistical information and aspects of student management

For many users, CeTARS serves as the gateway to 21 sub-systems or modules, all of which are accessed via CeTARS' homepage. A few of the programs accessed through CeTARS include: Catalog of Navy Courses (CANTRAC); Enterprise Navy Training Reservation System (eNTRS); Navy Training Quota Management System (NTQMS); Class Event and Resource Scheduler (CERS); and Recruit Training Management (RTM).

"CeTARS standardizes reporting at all activities that train Navy students," said David. "It allows training managers and upper echelons to support Navy training by maintaining accurate student, instructor and course data; all of which helps Navy leaders make informed decisions with the most current and accurate data available. With this new upgrade, we're operating in an even more standardized environment."

The new Navy training home page is: https://main.prod.cetars.training.navy.mil.

Users may experience a slight delay when accessing the new URL for the first time. The delay should be less than three minutes, in most cases. However, when accessing the CeTARS Discoverer tool, the delay may take three to five minutes, during which time a white screen will be displayed. After this, the login page should be normal.

If a user experiences a problem accessing the new CeTARS URL on a Navy-Marine Corps Internet (NMCI) computer, they should clear their computer's Java cache and remove the CeTARSII security certificate before accessing the new URL. Anyone continuing to experience problems or needing assistance clearing the cache should contact the NETPDTC helpdesk: at (850) 452-1001 or DSN 922-1001, then select option 1.

CeTARS supports more than 4,000 users, primarily training administrators and managers located at more than 300 locations worldwide. It also supports management and tracking of more than 1,000 courses with an average daily attendance of more than 50,000 students. CeTARS interfaces with 39 other applications and systems in the Department of Defense to share student data and order writing capabilities in support of MPTE enterprise efforts.

For more information about the Naval Education and Training Professional Development and Technology Center visit: https://www.netc.navy.mil/netc/Commands/NETPDTC.aspx.

Additional information on the Naval Education and Training Command can be found on the NETC website: https://www.netc.navy.mil/.

Information Dominance (N2/N6), Naval Intelligence Welcomes New Leadership

By Joe Gradisher, DCNO for Information Dominance Public Affairs

WASHINGTON, DC -- VADM Kendall L. Card assumed the duties of the Deputy Chief of Naval Operations (DCNO) for Information Dominance (N2/N6) and Director of Naval Intelligence (DNI) during a change-of-charge ceremony at the Pentagon, June 1.

Card succeeded VADM David J. Dorsett, who retired following a 33-year naval career.

Dorsett, the 63rd director of Naval Intelligence, assumed office as the first DCNO for Information Dominance in November 2009. Information Dominance is designated as the lead office for bringing the Navy's intelligence, cyber warfare, command and control, electronic warfare, battle management and knowledge of the maritime environment areas together to align oversight, governance and synchronization mechanisms to deliver end-to-end insight and accountability for Navy information requirements, investments, capability development and force development.

Under Dorsett's leadership, Information Dominance was elevated to a "main battery" in the Navy's arsenal.

VADM Kendall L. Card, DCNO for Information Dominance (N2/N6) and Director of Naval Intelligence

He also brought together more than 45,000 military and civilian professionals to form the Information Dominance community, tasked with building and operating this main battery.

"It has been the highlight of my career to bring the N2/N6 team and Information Dominance community together to allow the Navy to capitalize on the opportunities and face the challenges of the information age," said Dorsett. "I've been humbled by the dedication and creativity of the members of our team; they are leaders in a revolution in naval affairs that will assure the Navy is prepared to deal with the changing and growing threats ahead."

Dorsett was born in Roanoke Rapids, NC, and raised in Virginia. He graduated from Jacksonville University, Jacksonville, FL, in 1978. Following his qualification as a surface warfare officer, Dorsett was designated as a naval intelligence officer. He participated in numerous operations, including Southern Watch, Restore Hope, Desert Fox, Southern Watch Resolute Response, and other sensitive, nationally tasked combat and special operations. As a flag officer he served as special assistant to the Director of Naval Intelligence, Director of Intelligence, U.S. Pacific Command and Director for Intelligence, U.S. Joint Staff.

Dorsett graduated with distinction from the U.S. Naval War College and Armed Forces Staff College, with a master's degree from the Defense Intelligence College.

Prior to assuming the mantle of DCNO/DNI, Card was the Director of Concepts, Strategies and Integration for Information Dominance on the N2/N6 staff. He is a career naval aviator with more than 3,900 flight hours in the SH-3H Sea King, SH-60F Seahawk, and the S-3A Viking aircraft. He has commanded Helicopter Antisubmarine Squadron 15, USS Rainier (AOE 7) and USS Abraham Lincoln (CVN 72).

As a flag officer, Card has served as director, Command Control Systems, North American Aerospace defense Command and U.S. Northern Command; commander, task forces 51/58/59/151/158, Manama, Bahrain; and commander, Expeditionary Strike Group 3.

Card is a native of Fort Stockton, TX. He earned a Bachelor of Science in mechanical engineering from Vanderbilt University and holds a master's degree in national security and strategic studies from the U.S. Naval War College.

"It is an honor and a privilege for me to assume these duties," said Card. "I look forward to leading the N2/N6 and Information Dominance community teams as we face all future challenges."

VADM Card Qualifies for IDWO Pin

(Left) Deputy Chief of Naval Operations (DCNO) for Information Dominance/Director, Naval Intelligence (DNI) VADM Kendall L. Card receives his Information Dominance Warfare Officer pin from RADM David W. Titley, Oceanographer and Navigator of the Navy/ Director, Maritime Domain Awareness and Space, in a ceremony at the Pentagon. (Official U.S. Navy Photo)

(Left to right) RDML William E. Leigher (Information Warfare), RADM David W. Titley (Oceanography), VADM Kendall L. Card (DCNO/DNI), and RADM Samuel J. Cox (Intelligence), pose following the Information Dominance Warfare pinning ceremony for Card. Leigher, Titley and Cox represented their respective communities while serving as board members for Card's qualification. (Official U.S. Navy Photo)

Naval Academy Expands on Cyber Security Curriculum

By MC2 Alexia Riveracorrea, U.S. Naval Academy Public Affairs

ANNAPOLIS, MD -- The new academic year marks the beginning of the Naval Academy's new cyber security curriculum, in which midshipmen are required to take classes that will enhance their knowledge of cyber warfare and the threat it poses to national security.

Discussion of building a cyber curriculum at the academy began several years ago when the Chief of Naval Operations (CNO) explained the importance of cyber security to the Fleet, said CAPT Steven Simon, director of the academy's Center for Cyber Security Studies.

"The Department of Defense and the CNO identified cyber as an area that is critically important to all naval officers," said Simon. "When midshipmen get commissioned and go out into the Fleet, whether they are standing watch on a submarine, on the bridge of a surface ship, attached to a squadron or in the field, the decisions they have to make will be partly influenced by how the cyber domain impacts their ability to conduct their mission. These courses are meant to give them a foundation in cyber education."

Once the CNO put out the message, the academy initiated an examination of cyber security and how it should become a part of the curriculum at the Naval Academy, explained Associate Professor Christopher Brown of the computer science department.

"The academic dean assigned a committee to help create a report which outlined that cyber security was relevant to an academic setting like the Naval Academy and how it might be incorporated into the midshipman experience," said Brown.

As one of the contributors to the plan, Brown helped the coordination and development of the plebe year core course, SI 110, also known as "Cyber 1."

"The Cyber 1 course is basic general knowledge about how computers work, how networks are put together, and the vulnerability of those networks," said Simon.

The focus of this course is to increase the baseline and knowledge of cyber security for all plebes. When they get to the Fleet, they will be prepared, explained Deputy Director of the Center for Cyber Security Studies, CDR John Myers. From the beginning, he said the intention was for the course to be technical and hands-on.

"Ultimately, the students will do some network attacks as well as network defense," said Brown. "Along the way, they also will be able to modify some programs, produce some Web pages, build a wired or wireless network, and try to attack some websites."

The course consists of two hours of lecture and two hours of lab per week and is divided into three portions. "Cyber Battlefield" emphasizes the understanding of digital data, Internet protocols, the physical computer, operating systems, programs, Internet, wired networks and more. The second part is called "Models and Tools," in which the plebes will learn about protecting and attacking in the cyberspace through the use of theoretical models, said Brown.

"We look at some kind of theoretical model for what it is that you are actually trying to protect or attack in cyberspace, what are you defending, as well as general-purpose tools, including firewalls and cryptology that allows you to start protecting things," said Brown.

In the final part of the course, called "Cyber Operations," the students will put what they've learned up to that point to practical use.

"Here, they really take that knowledge to build, defend and attack other networks," said Myers. "We hope to create that baseline of cyber security for each of the plebes. Then in their junior year, they will take Cyber 2, which will allow them to have a much better understanding of cyber security."

"Cyber 2 goes into more depth and provides some background on policy and economics," said Simon. "From here on, there will be some elective type courses offered by different departments around the yard, so students who are interested can go deeper. But the baseline is to provide every midshipman that graduates this understanding of the cyber domain and how it impacts their commands and ability to conduct their missions."

The Center for Cyber Security Studies is designed to work interactively with academic departments around the yard to help develop cyber security courses and provide necessary expertise as the academy builds on its cyber program, said Simon.

"The idea is to work with the government and industry to broaden this, and bring more expertise into the yard so students gain more appreciation for it," he said.

It's becoming increasingly clear that cyber security is a real issue, particularly for military organizations but for individuals as well, Brown said.

"Learning these concepts and being able to make principled decisions in regards to security and your personal and professional life is really going to be important for these students when they graduate," Brown said.

USS Abraham Lincoln Passes First Underway Cyber Inspection

Compiled from USS Abraham Lincoln & CYBERFOR Public Affairs

USS Abraham Lincoln (CVN 72) passed a first-of-its-kind afloat U.S. Fleet Cyber Command Cyber Readiness Inspection (CCRI) July 14, while the ship was conducting training at sea.

A CCRI is an in-depth inspection and analysis of a ship or shore command's network security posture to ensure that vital information is protected from cyber attacks. According to the Navy Cyber Forces' (CYBERFOR) Cyber Security Inspection Certification Program (CSICP) training and assist teams the inspection also involves investigation of "authorized" USB usage, reviewing logs for authorized and unauthorized activity and making sure scan patch analysis have been updated.

"One of the most common violations we find in our inspections is discovering that someone has plugged their iPhone into a government computer," said LCDR Hezekiah Natta, assistant lead for CSICP's training and assist teams. "We also often learn that a ship/command is not in compliance with an Information Assurance Vulnerability Alert (IAVA), which is an announcement of a computer application software or operating system vulnerability notification."

Natta emphasized that these selected vulnerabilities are the mandated baseline, or minimum configuration of all hosts residing on the Global Information Grid (GIG). The Untied States Cyber Command (USCYBERCOM) analyzes each vulnerability and determines if it is necessary or beneficial to DoD to release it as an IAVA. "Implementation of IAVA policy helps ensure that DoD components take appropriate mitigating actions against vulnerabilities to avoid serious compromises to DoD computer system assets that would potentially degrade mission performance," said Natta.

The inspection of the Lincoln networks, which began July 8, marks the first time a cyber inspection of a Navy network was conducted underway, and the first DISA-led CCRI conducted aboard an aircraft carrier.

CDR Michael Thibodeau, the ship's combat systems officer, said the inspection was part of a three-year training cycle. The goal is to determine which DoD computer networks have low vulnerability to outside attacks from threats such as hackers, and to strengthen the defense of these networks as necessary.

"Networks out of compliance can actually be forced to shut down and pulled from the GIG," he said. "This success is indicative of Lincoln's high state of operational readiness."

Lincoln's inspection results set the Navy standard for afloat units by achieving a score 11 percent higher than had previously been achieved in shore-based inspections. Thibodeau added the ship's score was also 20 percent higher than the average afloat command score from the Navy's own internal cyber security inspections.

"I attribute our success on this inspection to the pride and dedication the Information Systems team takes in maintaining the highest levels of cyber readiness," he said.

Lincoln's next CCRI is not scheduled to occur until after Lincoln's upcoming Refueling Complex Overhaul (RCOH), as the ship will be temporarily taken off the training cycle.

Though the inspection is complete, IT2 Toni Robinson said personnel should continue to follow the practices that played a key role in passing the inspection.

"In order to keep prepared, all hands should remain vigilant on network security and follow command security procedures for personal electronic devices," she said.

Lincoln is currently working with other afloat units to help them prepare for success with their upcoming CCRI inspections.

"Our main function is inspections, but we also assist with training," said Natta. "The Navy's networks are our combat systems and we need to maintain and protect them like other military equipment."

LETTERS FROM THE GROUND

Greetings from Baghdad,

A group of 46 Cryptologic Technicians (CT's), Information Warfare officers and Army Signals Intelligence (SIGINT) Soldiers, deployed in support of Central Command, make up Request for Forces (RFF) 863.

This RFF provides manpower for the Joint Expeditionary Signals Intelligence Tactical Reconnaissance (JESTR) Detachment which conducts airborne – sound-to-go (A-STG) and ground – sound-to-go (G-STG), signals geo-location operations and other special purpose SIGINT missions in order to identify, track, target and provide actionable intelligence against terrorists and foreign fighters, anti-Iraqi forces, insurgents, militias and individuals associated with Improvised Explosive Device (IED) networks.

The preceding mouthful is simply a description of the group designed to assist in applying increased pressure against Anti-Coalition Forces through kinetic and non-kinetic targeting in support of United States Forces – Iraq (USF-I).

JESTR Detachment personnel also traditionally train and

Graphic Illustration by MC1(SW) Joshua J. Wahl

certify Army Division and Brigade personnel in the use and operational employment of G-STG systems as necessary.

The Navy component of the JESTR 'X' (10) team started their deployment last December. After the G-STG operator course in Fort Meade, MD, in January, they attended the Advanced Army Combat Training course in Fort Dix, NJ, and arrived in theater in March.

They wasted no time starting missions in support of Operation New Dawn after receiving certification to operate in country. Their tasking has demanded courage and flexibility as they repeatedly went into harm's way, deploying outside the wire, a total of 1,262 combat missions with Army and Air Force action arm elements. Their ability to remain vigilant while conducting combat operations in support of overseas contingency operations and the continued implementation of active force protection measures in order to deter, disrupt or prevent attacks against USF-I and Coalition forces has been a great success.

Official U.S. Navy Photo

An Iraqi woman and her daughter pose with CTR1(SW) Laurel Schwindenhammer.

To date, these operations have resulted in the capture of 39 high value individuals and ensured a continuous flow of real-time intelligence by answering 2,468 requests for information producing 540 target packages and 8,814 analytical products. This information increased multi-national tactical decision maker's situational awareness, while maintaining an accurate battlefield picture of terrorist networks and played a critical role in reporting the disposition of enemy forces.

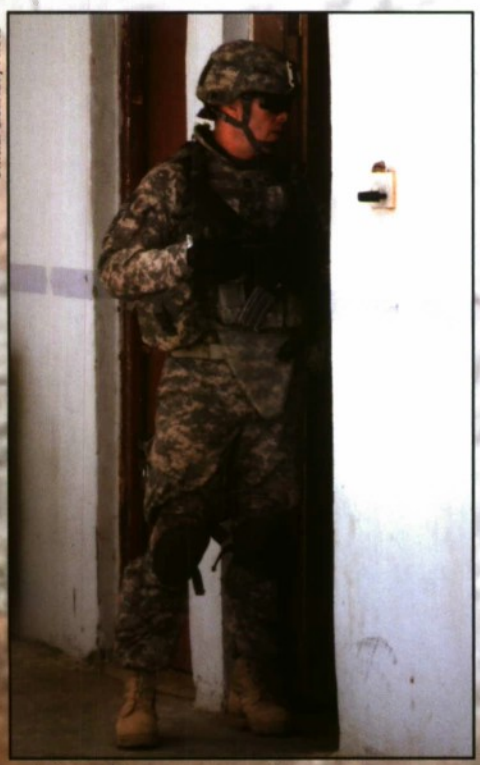
The detachment's ambitious approach to each mission has reduced the enemy insurgent's ability to operate effectively within USF-I's area of responsibility and has directly attributed to the reduced indirect fire against all forward operating bases. Their technical knowledge is incorporated daily by Task Force Battery Commanders, Battalion S2's, and United States division collection managers for proper employment of G-STG tactics, techniques and procedures.

In addition to their primary mission, the JESTR Detachment teams have integrated themselves into their respective platoons to provide boots on ground security support. JESTR X's willingness to spend countless hours engaging local Iraqi citizens in support of Information Operations campaigns, as well as advise and assist brigades and security advisory patrols enhances both security and stability in an environment that had been historically hostile towards U.S. forces.

With the future of Iraq in the hands of its citizens and with U.S. forces leaving, the JESTR Detachment is methodically shutting down their operations throughout Iraq and redeploying to conventional Navy and Army billets from October through December 2011. These service members are the second to the last active G-STG and last A-STG elements in Iraq and have flourished in non-traditional service roles.

Of note, during their deployment, these Sailors and Soldiers have received a variety of awards including, but not limited to the Iraqi Campaign Medal, Army Combat Action Badge, Navy Combat Action Ribbon, Expeditionary Warfare Insignia, the Bronze Star, the Air Medal, and the Army Commendation Medal.

This deployment is a testament to Sailors, Soldiers and Airmen working side-by-side to achieve mission success.



Official U.S. Navy Photo

CTRCS(SG/SW) Patrick Wolfrey clearing a room.

Official U.S. Navy Photo

(Left to right) U.S. Army Capt. Baker, CTRCS (SG/SW) Wolfrey, Army 1stLt. Sommer and CTR1(SW) Schwindenhammer preparing to hit the road.

CIO's Network Tips

NM Encourages Computer Restarts

By LCDR Paul Dreher, FLTCYBERCOM

EDITOR'S NOTE – *Mild Mannered Mike (M3) has many years' experience from the early days of computers and is a recognized leader in the field of Information Technology and Cyber Security. M3 is known for practical IT solutions when it comes to dealing with the daily problems experienced in today's high tech environment. When confronted with inexperience, apathy or bad practices, he transforms into his alter-ego 'Network Man' who lives by the philosophy that if you give a person a fish you can feed him for a day, but if you teach him to fish you feed him for a lifetime.*

CDR Jones, the Weapons Officer, is complaining about his computer. He is frustrated with slow operation and poor response. "I just don't know what's going on with my computer," said Jones. "It's so slow and getting slower every day! What's going on? I can't get my work done!"

M3 is nearby shredding documents when he hears Jones venting his frustrations. Hearing this, M3 transforms into Network Man!

"How long have you been experiencing these computer problems?" Network Man asks.

"It started a few months ago. I ran a virus scan at the time, but nothing was reported," Jones responds.

"When was the last time you restarted the computer?" Network Man asks.

"It's been a month or two. Besides, why would I do that?" asked Jones. "The computer is slow enough as it is. I'm very busy and I don't have time to wait for it to start up again!" he angrily adds. "And I understand the commanding officer is having the same problem!"

"Restarting your computer on a nightly basis has many benefits," Network Man explains. "First, it clears out the memory because many programs don't release all the memory they've used when you exit the program. This means less memory is available for other programs which reduces performance. Also, restarting allows software patches to finish installing. If the updates aren't installed, your computer won't be fully guarded against new threats. Additionally those patches will continue to take system resources until they finish. Let's walk through this."

After restarting the computer, several patches and updates are installed and Jones' computer is back to normal.

"Just remember, when you head home each day, simply select 'Restart' instead of logging off," Network Man said. "That way, your computer will be restarted and ready to use when you return the next morning. Also, never just lock the computer at the end of the day – that's a real security issue. And remind your watchstanders restart their computers during watch turnover once every 24 hours."

"I never knew...," Jones said as he waved goodbye. Finally, he was able to get back to work.

For additional information on restarting your PC, contact your Information Assurance Manager (IAM) or refer to Navy Telecommunications Directive (NTD) 06-11 Navy Network Discipline.

If you have questions or suggestions for Network Man, contact Toni Turbide at:

NETWARCOM_LTLC_CIO_NETWORK_INTEGRATION@navy.mil.

738th AEAG Sailors Perform Intelligence Advising Mission

By Capt. Jamie Humphries, USAF, 438th Air Expeditionary Wing Public Affairs

KANDAHAR, Afghanistan -- Two Sailors assigned to the 738th Air Expeditionary Advisory Group (AEAG) at Kandahar Air Wing (KAW) work hard to keep aircrew out of harm's way while advising Afghan intelligence analysts.

Meet U.S. Navy IS3 Armando Rodriguez and IS3 Steven Schuyler, 738th AEAG.

The two Sailors work as Air Intelligence Advisors with Afghan Air Force (AAF) intelligence experts at KAW. Along with seven other Sailors, they make up a small Navy contingent which works daily with U.S. Air Force members to advise the AAF.

The crew--along with intelligence analysts Belgian Adjutant Phillip Sacre and U.S. Air Force Maj. Jimmy Jacobson, USAF, 738th AEAG -- are charged with providing operations group intelligence support, threat and intelligence analysis, updating group leadership of potential threats, maintenance of all applicable reports, and most importantly, training the AAF intelligence unit.

(Left to right) IS3 Armando Rodriguez and IS3 Steven Schuyler, 738th AEAG, work as Air Intel Advisors with AAF intelligence experts at Kandahar Air Wing. They make up a small Navy contingent working daily with USAF members to advise AAF members with a goal of Afghans being able to operate their own independent AAF. (USAF Photo by Brian E. Christiansen)

Group Support:

A typical day involves arriving at the intelligence mission planning cell 90 minutes before each scheduled Afghan Mi-17 helicopter flight. The analysts provide a current threat assessment to the aircrew. This includes a brief on the location of travel, potential threats along planned routes and critical information discovered in daily threat reports.

Aircrews are made up of Americans, Lithuanians and Afghan members. Although language barriers provide a challenge during pre-flight briefs, intelligence experts agree they have seen a dramatic change in the Afghan ability to exchange information.

"One big change is that the AAF flight crews are now discussing maneuvering and threat avoidance during our pre-flight brief," explained Schuyler, originally from Muncie, IN. "They now talk about threats along the routes and are communicating, which is a good thing."

After the pre-brief, the analysts issue communication equipment needed to ensure crews have the necessary tools needed in case of an emergency. One piece of issued equipment is a traveling beacon known as "Blue Force Tracker". The tracker is used as a locating device to give intelligence experts an exact pinpoint of where the Mi-17 helicopter and crew are at any given moment. They also issue a satellite phone that can be used to discuss important information as well as a booklet with helicopter landing zone cards, imagery of all helicopter landing zones and list of potential flying hazards and frequencies. Experts explain their aim is to provide a common operating picture of the landscape and terrain while maintaining safety of the crew.

"Our goal is to keep aircrew and aircraft safe. It's very important we teach the AAF now where and why to fly so they can return here unharmed," said Rodriguez.

Advising Mission:

When not performing the operational mission, the intelligence unit works to train AAF intelligence advisees. Each member of the AAF team begins training at the Basic Air Intelligence Course in Kabul before transitioning

. . . continued on Page 16

to Kandahar. The intelligence airmen in Kabul provide initial training by building training folders for the Afghans and each airman must demonstrate completion of basic level-three training before transitioning to KAW. When they arrive, the analysts in Kandahar review and assess the advisee's weaknesses and work with them to strengthen those areas.

"We're very fortunate; we see the progress in front of our faces and we see them learn," said Rodriguez, a native of Jacksonville, FL. "The AAF members we have here are working for their jobs and for their country. The motivation is there. We can see it."

To avoid complacency in the training environment, the advisors switch off week to week between training and operations, teaching the Afghans basic map reading skills, how to navigate routes, plot points and pull points on a map has increased the mission, said Schuyler. Being able to point to a location on a map and having them come up with latitude and longitude is great progress.

Although progress is being made, there are still deficiencies the team is working to overcome. Because of the relative newness of intelligence agencies in Afghanistan, it's still somewhat difficult for Afghans to share information, Schuyler said.

"We also have motivated Afghans who work here with us, so it's hard to keep them here to work with us for an extended period of time," he said. "On occasion, they may be pulled to perform other duties simply because they've demonstrated the ability to excel."

Despite the high-operations tempo already displayed at the intelligence unit, the crew is about to get even busier with the possible arrival of AAF C-27s. Due to the fixed-wing aircraft's greater reach, the analysts will now have to assess a greater area than they typically do with helicopters.

"We primarily focus on regional command south and southwest," said Schuyler. "C-27s will greatly expand our area of responsibility and coverage area."

Despite all the challenges, if anyone can handle the uniqueness of working in a different environment, it's Rodriguez and Schuyler who both grew up in Navy families. Rodriguez's father, ATCM Armando Rodriguez, is still on active duty and assigned to the Amphibious Assault Ship USS Boxer in San Diego, while Schulyler's father is a retired Sailor.

"Joining the Navy is what I wanted to do," said Rodriguez. "I've learned a lot here and it's been a great experience."

GNOC Detachment Manager Completes DoD's Executive Leadership Development Program

By Roger D. Williams, Administrative Director, GNOC Detachment, Norfolk

NORFOLK, VA -- Naval Network Warfare Command, Global Network Operations Center Detachment Norfolk's Kevin Sturlaugson of NetOps 3 recently graduated from the Department of Defense (DoD) Executive Leadership Development Program (ELDP).

Official DoD Photo

While alongside Marines, ELDP personnel got a taste of the 'Crucible' - the final test that must be passed before a recruit can become a Marine. The Crucible tested participants' abilities to overcome physical challenges and fears, and to trust in others.

Sturlaugson was selected from a field of more than 750 applicants to be one of just 51 participants in the 2011 DoD ELDP class.

This high-visibility, cutting-edge program took its participants literally around the world to learn in academic and tactical environments about a broad variety of programs and operations throughout active-duty and civilian components of DoD.

The program is a challenging 10-month series of intensive training evolutions, seminars and exercises at DoD bases, headquarters and facilities throughout the United States, Asia and Europe. The ELDP management office states that the program is mentally and physically challenging, providing intense, hands-on field experience for high-potential individuals.

Official DoD Photo

ELDP participants learned the importance of teamwork to success, as they trained with some of the world's most elite warfighters - Navy SEALs - on the sands of Coronado, CA.

Sturlaugson and his classmates immersed themselves in the field with warfighters, experiencing such activities as the Marine Corps' Crucible, rappelling 72-foot towers with the Army, observing the operations of the DoD's POW/MIA recovery teams, and witnessing the tension-filled environment at the DMZ dividing North and South Korea.

Additionally, the group engaged in rigorous academic studies, technical research and doctrinal development - all designed to help them gain a greater understanding of the key programs, processes and policies of DoD and its domestic and international impacts.

While the numerous deployments, direct involvement in combat training and strategic activities, and seemingly endless time conducting DoD-related research were invaluable components of the program, Sturlaugson said he benefited tremendously from his yearlong interaction with counterparts at duty stations across the country, working for the various U.S. military services.

Official DoD Photo

At the Ranger Malvesti Field Obstacle Course, Fort Benning, GA, program participants challenged their fears and tested their physical abilities.

"The Department of Defense is more than a group of warfighters maintaining this country's freedoms and helping our allies preserve theirs," said Sturlaugson. "It's also thousands of caring people who unhesitatingly provide humanitarian aid around the globe for those who are facing tragedies."

Following his return to Norfolk at the end of the program, Sturlaugson declared DoD ELDP to have been one of the most significant parts of his 21-year combined active duty and civilian career with the Navy. He not only felt honored to have been able to participate in such a premier program, but he also is confident that its lessons will markedly enhance his ability to perform professionally and support his mission - regardless of what current and future assignments he may face.

"This country's warfighters deserve the best possible support, which can only be achieved through knowledge and teamwork - which I gained by participating in this outstanding program," said Sturlaugson.

The DoD ELDP is open to government civilian personnel in grades GS-12 through GS-14, as well as active duty O-3 or O-4 personnel from all branches of the military. Further information on the program, including eligibility requirements and application instructions, is available through the DoD EDLP Office at (703) 696-9633, or at http://www.cpms.osd.mil/lpdd/eldp_index.aspx.

Stories & Photos by George Lammons, NMOC Public Affairs

Bowditch Completes Surveys in Vietnam

Oceanographers from the Stennis Space Center-based Naval Oceanographic Office (NAVOCEANO) finished a month of surveys off the Vietnam coast looking for Vietnam era U.S. military losses in underwater environments.

The team of 12 oceanographers and hydrographers from NAVOCEANO on board USNS Bowditch (T-AGS 62), an oceanographic survey ship, conducted the surveys from May 20 through June 20 for the U.S. Joint POW/MIA Accounting Command and the Vietnamese Office for Seeking Missing Persons.

RDML Jonathan White, commander of the Naval Meteorology and Oceanography Command (NMOC), and Bowditch Master, CAPT Mike Farrell, co-hosted a reception in Da Nang, Vietnam, on board Bowditch to mark the end of the survey portion of the mission.

NMOC, based at Stennis Space Center, is NAVOCEANO's parent command.

Gough Leaves Naval Meteorology & Oceanography Command

Edward C. Gough Jr., deputy/technical Director of the Stennis Space Center-based Naval Meteorology and Oceanography Command (NMOC), left the command to become Senior Principal Scientist at the NATO Undersea Research Center (NURC) in La Spezia, Italy.

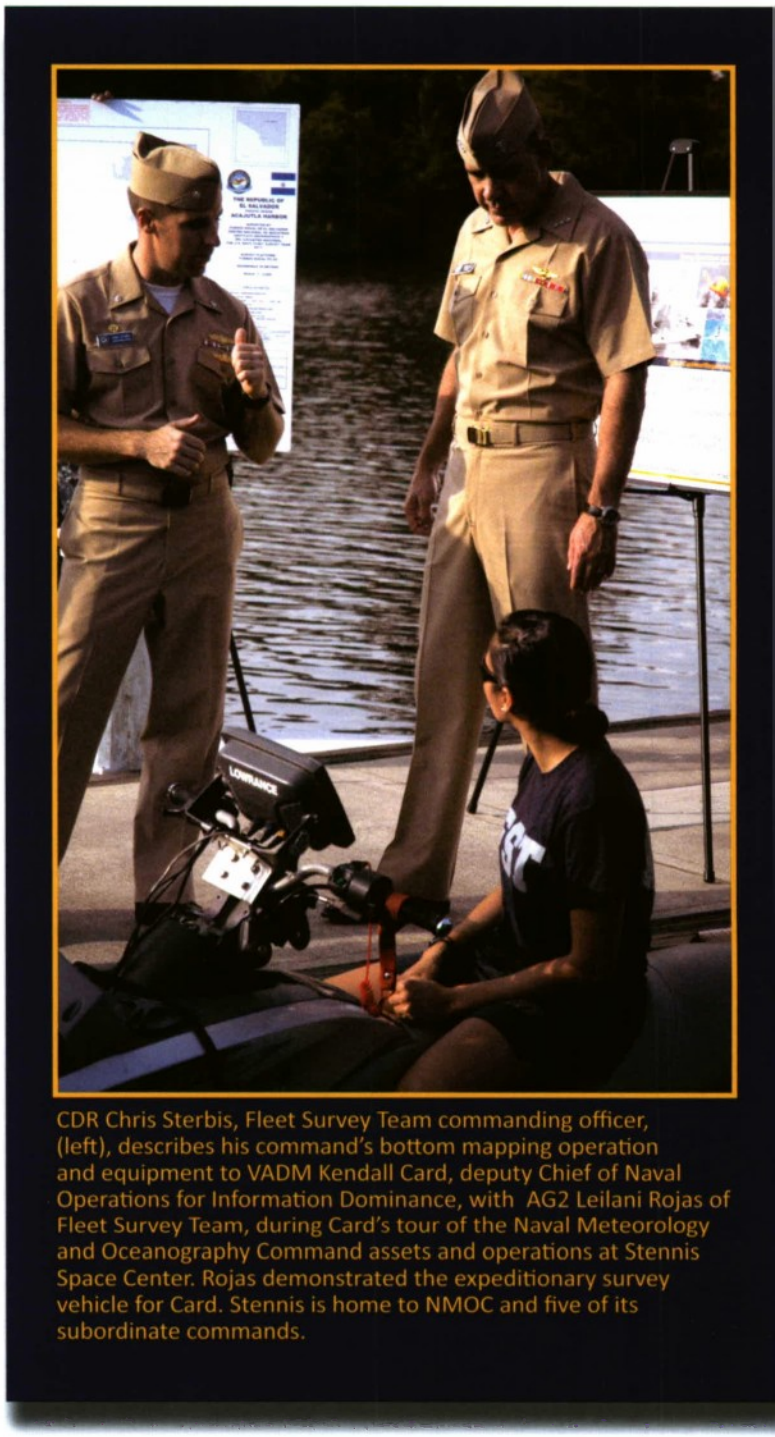
Gough, joined the command in 2003 after serving as Science and Technology Advisor to the commander of the U.S. Pacific Command in Hawaii.

FNMOC Concludes Support for the Space Shuttle Program

The launch of the final space shuttle mission marked the end of 23 years of shuttle mission support from the Monterey, CA - based Fleet Numerical Meteorology and Oceanography Center (FNMOC).

Since 1988, FNMOC has supported every shuttle launch with crucial weather and ocean prediction. The predictions included significant wave height, primary wave period and direction, sea surface temperature, and marine winds in the splashdown area for the solid rocket boosters.

"This information provided the booster recovery team with vital ocean information in preparation for and during their recovery efforts," said Sue Uhrich, head of the FNMOC shuttle support effort since 1997. "If wind and sea conditions predicted by our models exceeded the limits for safe recovery of the solid rocket boosters, the shuttle launch would be scrubbed."



CDR Chris Sterbis, Fleet Survey Team commanding officer, (left), describes his command's bottom mapping operation and equipment to VADM Kendall Card, deputy Chief of Naval Operations for Information Dominance, with AG2 Leilani Rojas of Fleet Survey Team, during Card's tour of the Naval Meteorology and Oceanography Command assets and operations at Stennis Space Center. Rojas demonstrated the expeditionary survey vehicle for Card. Stennis is home to NMOC and five of its subordinate commands.

Maritime Function Transfers to San Diego, Completing Center Establishment

Naval Maritime Forecast Center, Pearl Harbor (NMFC-PH) transferred the last of its maritime forecasting functions to Fleet Weather Center San Diego (FWC-SD), marking the final phase in the establishment of the San Diego center, three months ahead of schedule.

FWC-SD commemorated the transfer with a ribbon cutting ceremony July 15 and achieved its Initial Operating Capability (IOC) as a result of the transfer.

"Third Fleet geographic area spans from the California coast to the International Dateline, from the North Pole to the South Pole," VADM Gerry Beaman, commander of U.S. 3rd Fleet, said at the ribbon-cutting ceremony. "I depend on people like you, working in facilities like this, to continually collect data, aggregate that information, and help me achieve decision superiority."

The transfer had been in process for more than a year, but the turnover took eight months. The transfer of function was originally scheduled for September, but the shift occurred on June 15.

FWC-SD built a new watch floor, brought online vital communications systems, and implemented a robust training program to ensure all incoming personnel met the rigorous watch position standards.

Additionally, FWC-SD assumed its new responsibilities in a phased approach -- 3rd Fleet in October 2010; 5th Fleet products in February 2011; 7th Fleet responsibilities in May 2011. The final piece of the transition occurred June 15 with the move of the Ship Routing Officers (SROs) from NMFC-PH to San Diego and the assumption of the Optimum Track Ship Routing (OTSR) mission.

The FWC-SD, based at Naval Air Station North Island, provides full-spectrum weather services to land, sea and air naval units and contingency exercises and operations to facilitate risk management, resource protection and mission success of Fleet, Regional and individual unit commanders.

NAVO Dedicates New Computer Center

The Naval Oceanographic Office (NAVO) at Stennis Space Center, MS, held a ribbon-cutting and dedication ceremony on May 12 for a state-of-the-art, 2,800 square foot computer facility.

The Dan H. Williams Oceanographic Information Technology Center will host Information Technology (IT) assets, including High Performance Computing, virtual clusters, the NAVO web presence and data collected over the past 40 years. NAVO's data holdings total approximately one petabyte of irreplaceable oceanographic data. The facility will serve as the central NAVO IT hub and data repository for years to come.

FNMOC Conducts 50th Anniversary Celebration & MILCON Ribbon Cutting

More than 250 people gathered at Fleet Numerical Meteorology and Oceanography Center (FNMOC) in Monterey, CA, May 19 to celebrate the organization's 50 years of excellence and to cut the ribbon signifying completion of its recent military construction project.

The ribbon-cutting ceremony featured speeches by Monterey-area military dignitaries, historical exhibits, tours of the computer center and 30-minute panel discussions – Fleet Numerical of the Past, Fleet Numerical of the Present, and Fleet Numerical of the Future.

STENNIS SPACE CENTER, MS -- AGCM Keith Edwards (center), command master chief of the Naval Meteorology and Oceanography Command (NMOC), cut the aerographer birthday cake with AGAN Tara Flaugher of Fleet Survey Team and AG1 Scott Belt of Navy Oceanography Anti-Submarine Warfare Command. The youngest and oldest of assembled aerographer's mates stationed at Stennis Space Center look on before their morning run. Jul. 1 marked the 87th birthday of the AG rating.

Pensacola Leaders Visit CID Corry Station

Mayor Hayward Calls CID a Military "Quiet Giant"

Story & Photo by Gary Nichols, CID Public Affairs Officer

PENSACOLA, FL – The veil of secrecy surrounding the Center for Information Dominance (CID) Corry Station was lifted a bit when several community leaders visited the learning site in July.

The guests included Pensacola Mayor Ashton J. Hayward; Commander, Naval Education and Training Command (NETC) RADM Joseph F. Kilkenny; retired ADM Robert J. Kelly, and several staff members from the University of West Florida and Pensacola State College.

This visit to Corry Station was a first for Hayward, who was sworn into office in January.

Commuters who travel the busy streets near Naval Air Station Pensacola pass Corry Station each day, but few have ever been on the base. And, fewer still know about the classified cryptologic and information systems training now being taught at CID Corry Station.

With a staff of more than 1,050 military, civilian and contracted staff members, CID Corry Station oversees the development and administration of more than 168 courses at 16 learning sites throughout the United States and Japan. CID Corry Station provides training for more than 19,000 members of the U.S. and allied Armed Services each year.

For 83 years, Corry Station has prepared Naval Aviators and Sailors to defend the United States.

The brick hangars that once housed the planes that helped train World War II fighter pilots have been transformed over the decades into secure compounds surrounded by a chain-link fence and armed guards. The classrooms and labs in these secure compounds where future cryptologists and information systems technicians learn the vital skills they will need to protect and defend the nation's computer networks are equipped with the latest state-of-the-art equipment.

Kilkenny explained that CID is somewhat of a mystery to the general public since not much is known about Corry Station's classified curriculum.

"The purpose of today's visit is to try and get the local community leaders to get a better understanding of what we do at Corry Station, particularly at the Center for Information Dominance," Kilkenny said. "We wanted to give them a tour of the facility so they can see some of the really revolutionary training that's going on here."

CID Commanding Officer CAPT Gary Edwards said the overall goal of CID is saving lives, and how CID meets that goal is by training the next generation of cyber warriors.

"Our challenge is an interesting one, not necessarily unique, but interesting," Edwards said. "In less than six months we are tasked with taking everyday citizens, most of them no older than 18 or 19, with various degrees of experiences and exposure, and train them to become information warriors; experts who are trained and ready to protect, attack and exploit the information domain."

Change is the one constant Edwards must deal with. He estimated that on average, information systems change about every 18 months.

"I do think our challenge is compounded by the need to stay ahead of technological advances," Edwards said.

Because of that unique factor, his Sailors must not only master technology and information systems, they must also become adept at critical thinking and problem-solving.

Several programs being taught, developed or tested at CID help the Navy stay ahead of the ever-changing technological landscape: Joint Cyber Analysis Course (JCAC), Information Systems Technicians of the Future (ITOF) and Digital Tutor (DT).

Joint Cyber Analysis Course

As a direct result of the increased cyber threat, in 2008 then-Secretary of Defense Robert Gates directed that an increased emphasis be placed on cyber training. Gates directed that cyber training at CID increase from 400 to 1,000 service members per year.

Consequently, CID completely overhauled its basic cyber training. A series of digital network analysis courses, (apprentice, journeyman and master-level courses) were combined and expanded. The course length was also increased to 24 weeks.

Not only does JCAC teach students the fundamentals and theory of information systems operations, students learn to think logically and analytically, and master a significant body of knowledge to tackle very complex problems.

This training facilitated technical growth that can combat current threats, provide flexibility to address future requirements and meets the National Security Agency (NSA) standard for basic entry-level technical analyst for Computer Network Operations (CNO).

Information Systems Technicians of the Future

George Trice, CID special programs officer, who presented the ITOF brief, said the acronym is actually a misnomer now because the course has been integrated into the CID curriculum, which is being taught now.

"Although we still refer to the course as ITOF, it's actually the Information Systems Technician of

Today," Trice said.

The ITOF program provides information superiority for the warfighter by aligning Navy IT training with Department of Defense 8570.1M Directive Certification Standards.

"One of the unique aspects of the ITOF course is that all students who successfully graduate from ITOF will have earned three computer-related industry standard certifications," Trice said. "This is the first Navy school that requires students to take professional certification exams as part of their course of instruction."

ITOF students receive nine weeks of training and test for professional certifications in COMPTIA A+ and Microsoft Certified Professional in Windows XP Operating System. Additionally, students complete three weeks of Cisco Certified Network Associate training, resulting in Sailors being fully developed as Information Systems Technicians, certified and ready to adapt to accelerated growth of Information Technology (IT) systems.

Digital Tutor

In 2007 the Defense Advanced Research Projects Agency (DARPA), based in Arlington, VA, coordinated with the Department of the Navy, through NETC, to conduct a four-year test to determine the feasibility of Digital Tutor, an experimental computer-based teaching system, at CID.

DARPA, an agency of the Department of Defense, was established in 1958 to prevent strategic surprise from negatively impacting U.S. national security and create strategic surprise for U.S. adversaries by maintaining the technological superiority of the U.S. military.

The four-year project is using the Information Systems Technician "A" school at CID for its test model due to the complexity and technical nature of the rating.

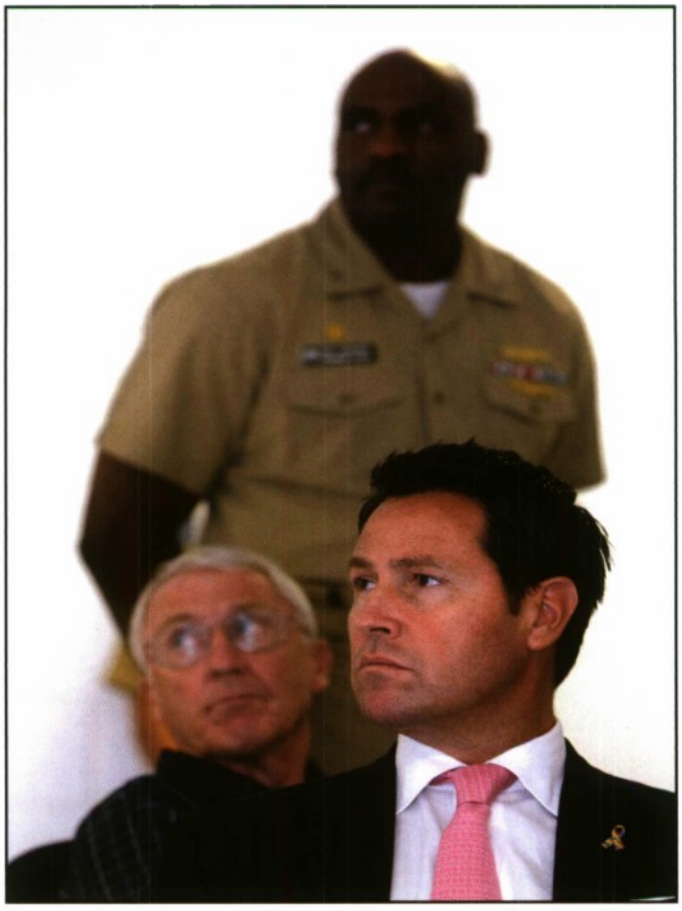
Now in its second phase of research, DT is an innovative and unique curriculum delivery system employing an adaptive motivational feedback process. If successful, DT will help produce, within 16 weeks, a journeyman-level technician who has the equivalent knowledge base of an IT with five to 10 years of actual experience in the fleet.

A 16-week DT course began in August as part of the final phase of testing with a second course starting in October.

The DARPA Executive Steering Committee decision on the outcome of DT is scheduled for October 2012.

Hayward noted that until his tour at Corry Station, he had been largely unaware of the scope and importance of the mission at CID.

"Corry Station has always been one of the 'other' bases in Pensacola," Hayward said. "After touring the facility and learning about the mission, I can truly say that Corry Station is one of the quiet giants of our military. In this modern age of electronic, cyber warfare, when information and technology can make the difference between winning and losing, Corry Station is leading the way by training America's next generation of cyber warriors."



(Front to back) Pensacola Mayor Ashton J. Hayward, retired ADM Robert J. Kelly and CID Commanding Officer, CAPT Gary Edwards.

Edwards estimated that in a five year period from 2008 to 2013, the Navy will have invested about $132 million in increased staffing and rebuilding of the Corry Station infrastructure.

"As a direct result of our attempts at staying ahead of technology, combined with increased requirements by the Department of Defense for cyber warriors throughout the fleet and the joint services, CID has had to invest heavily in increased numbers of instructors and staff, facilities upgrades and new construction," Edwards said.

This increase in training requirements translates directly into economic growth for the Pensacola area due to the increased need for additional instructors, along with upgrades to existing buildings and new construction of barracks and a gymnasium over the next several years.

"From a local government perspective, we are incredibly proud of our military bases, and CID Corry Station is an excellent community partner," Hayward said. "The high-tech mission and training applications serve our country but also create opportunities for private sector spin-offs that create good jobs in the area. Also, by expanding their facilities, Corry Station will boost our local economy and allow us to improve our community's infrastructure and quality of life. This was a great visit and I will rest easier knowing that our nation's 'shadow warriors' are on the job and here in Pensacola."

CID Learning Site Yokosuka Sailors Join Ishinomaki, Japan Relief Effort

Story & Photos byTrisha Pair, CID Learning Site Yokosuka, Japan

Nearly three months after the great Tohoku earthquake and tsunami devastated Japan, a group of Sailors, family members and contractors from Center for Information Dominance (CID) Learning Site (LS) Yokosuka, Japan departed for Ishinomaki, Japan to assist in the relief efforts in the affected region.

The group included CTT1(SW) Steven Olson, IT1(SS) Christian Pair, FT1(SS) Michael Wendell, James Amyx, Wilson Steiger and Trisha Pair.

DAY ONE ...

The drive to Ishinomaki took approximately seven hours heading northeast of Yokosuka Naval Base

One of the first things the group noticed was the overwhelming smell -- a stench of tidal remnants, rot and decay that permeated the city. Words could not adequately describe all the sights and smells experienced by the relief workers.

The group met four other members of the volunteer team including their team leader, Danny Furukawa.

Their quarters were on the second floor of a reclaimed storefront with no electricity. A small generator was available, which they only used a couple of hours each day for recharging cell phones and limited laptop use. There were restrooms with latrine style toilets only. The kitchen consisted of a propane stove, a few shelves and a sink

Each volunteer claimed a spot on the floor, laid out their sleeping bag and mat, and then set out to survey the surrounding devastation. Within walking distance from the camp they found a local ramen shop that recently reopened. They stopped in for dinner, chatted with the owner and some residents, then returned to the storefront to get some rest.

To re-emphasize the reality of what residents have been living with the past three months, at 12:40 a.m. the group was violently awakened by a 4.7 magnitude earthquake.

DAY TWO ...

After a light and uncomfortable sleep, the volunteers awoke at 6 a.m. to ready themselves for the day's tasks -- to prepare and distribute food to some of the displaced survivors.

Upon arriving at a local middle school/shelter, they met more volunteers – a physical education teacher and four of his students who had driven approximately six hours from Chiba University earlier that morning.

A bus full of food, supplies and more volunteers from Sakuragi Christian Center pulled up to the school. They supplied everything needed to make 1,500 servings of a traditional Japanese stew called Tonjiru (pork, tofu, miso and vegetables), with rice.

The next three hours were spent preparing the stew in 11 huge pots and continuously making rice using eight commercial rice cookers.

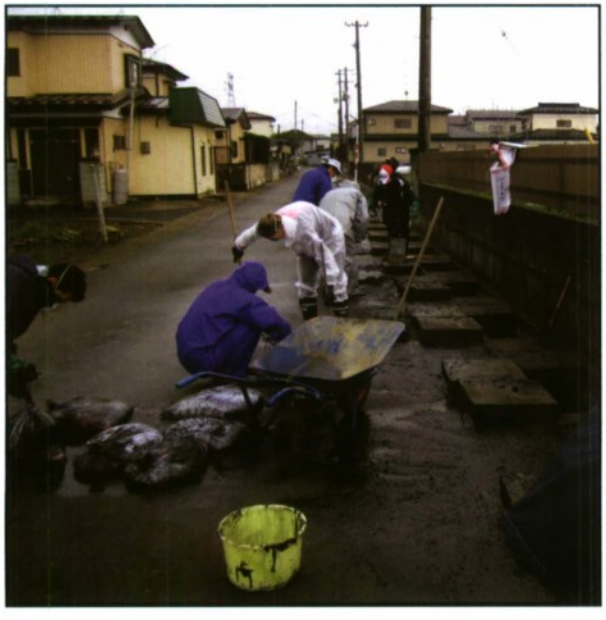
Once the food was prepared, it was transported and distributed it to three different shelters: the middle school where it was prepared, a neighboring high school and a nearby community center.

Once everyone in the shelters had been fed, the leftovers were taken to the nearby communities where people flocked to the back of the van for a hot meal.

Many people still had no gas or electricity, making any kind of hot meal a rarity.

The shelter's residents slept on small mats and used cardboard boxes for their few remaining possessions. The boxes doubled as borders between neighbors adding a sense of civility. The volunteers slept this way for one night and were already sore and exhausted from an uneasy rest. The survivors had been doing this for almost three months and still managed to find smiles and hope.

(Opposite Page) CID LS Sailors and other volunteers pose for a group shot after completing their 4-day adventure. (Below) Volunteers clean storm drains and load mud into sand bags before hauling them away. (Right) Volunteers survey damage on Nakaze Island months after the tsunami. The fuel tank in the background was swept approximately 300 feet from its foundation.



That evening, the volunteers were able to take their first hot bath since arriving. The Japan Maritime Self-Defense Force (JMSDF) had set up a traditional Japanese bathhouse in the neighborhood.

The CID volunteers went back to the small ramen shop that they had found on the first night. This time friends from Chiba University joined them. The owner of the shop was happy to see all, and they were able to get to know everyone a little better.

Later that night, all were awakened by another earthquake and several loud lightning crashes.

DAY THREE ...

This day's project was located at the home of two siblings in their late 80s and early 90s.

The rain gutters that line the streets are about 18 inches deep and are covered by large concrete blocks weighing about 80 pounds each. These blocks had to be individually removed for clearing out any debris and cleaning up buildup.

The tsunami had filled the gutters with heavy muck and debris that had settled since the water receded. Every time it rained, the gutters would back up and cause more flooding.

Each citizen is responsible for maintenance of the gutters that line their property, so the city had given this family a deadline to have them cleaned out to avoid incurring fines.

Volunteers began by shoveling the muck onto the street to let some of the rainwater drain before bagging the debris, despite a harsh and pungent stench. They removed all sorts of debris including car headlights and cell phones.

Throughout the day, the owners provided the volunteers with plenty of food and refreshments. They told stories about the day of the earthquake and tsunami. The floodwater lines on their home were still there and measured more than five feet high. They recalled surviving for four days on the second floor of their house, waiting for the water to recede.

During one of their breaks, announcements came over the loud speakers used for the emergency warnings, notifying all that it had been exactly three months since the great tragedy here in Japan. The entire city, including all of the volunteers, observed a moment of silence.

At the end of the day, the volunteers had moved more than 300 bags and 1,000 pounds of a putrid mixture of mud, decay and debris. Flow was restored to the gutters and the street was cleaned of any leftover dirt and mud.

Last but not least, the ground was leveled where vehicles had been pulled from their yard.

On their final night in Ishinomaki, the CID volunteers were joined by the entire team for a Sayonara Party at the ramen restaurant. The restaurant didn't have menus yet, so everyone just enjoyed whatever was placed in front of them. Some dishes were recognized and some not.

Everyone sang karaoke in both English and Japanese and were told that this was the happiest night they had experienced since the earthquake and tsunami had devastated the country.

The volunteers were humbled to realize that they had made a difference during their time off. Bringing back a sense of normalcy and supporting the local economy was an unexpected way to support a country they have all grown to love.

DAY FOUR ...

The next morning the volunteers packed their things and loaded the van for the long ride home.

Before leaving the area, they decided to drive around a little more. The devastation was even more overwhelming than earlier realized. Many areas hadn't even been touched yet, and coastal areas continue to flood every time the tide comes in.

One thing each volunteer had learned about the Japanese is that they are a strong people and will rise to the challenge. The volunteers accomplished so much in such a short time, but still there was much to do.

Meet your Naval OPSEC Support Team

By James Magdalenski, Director
Naval OPSEC Support Team

Photo by Robin D. Hicks

Naval OPSEC Support Team members (l to r): GySgt. Charles Wolf, Lee Case, James Magdalenski (Director), CWO3 Chris Pegram and Robert "Scott" Carey.

Department of Defense (DoD) Instruction 5205.02 dated March 2006 requires each service establish an Operations Security (OPSEC) support capability. As a result, the Naval OPSEC Support Team (NOST), located at Navy Information Operations Command (NIOC) Norfolk, is designated the Naval OPSEC support element, providing OPSEC support throughout the Navy and Marine Corps.

The NOST mission is to provide command OPSEC program development, awareness resources, assessment assistance, guidance and training that promotes an understanding of OPSEC among all service personnel and family members. The NOST supports these programs worldwide through several Websites, reach back capabilities and on-site subject matter expertise.

Located in building U-132 at Naval Station Norfolk, the NOST provides the following:

-- Two-day OPSEC Officer Course (J-2G-0966)

Taught monthly, this course alternates between NIOC Norfolk and NIOC San Diego. Mobile Training Teams are also available upon request and require a minimum of 12 students. The course covers the five-step process and illustrates the process through practical exercises, OPSEC officer program development and responsibilities, assessments and surveys, and internet-based capabilities (IbC).

-- OPSEC assessment, survey and assist visit support

OPSEC assessments are required annually. The DoD, in partnership with the Interagency OPSEC Support Staff (IOSS), contractors and the service OPSEC support elements, developed the web-based Operations Security Collaboration ARchitecture (OSCAR) risk assessment tool. Hosted on the classified network, OSCAR allows even the novice OPSEC Officer the ability to step through the assessment process and provide a consistent and technically sound methodology to identify, analyze, quantify and communicate risk. Request an OSCAR account at https://oscar.dtic.smil.mil/oscar.

-- Various OPSEC briefs

OPSEC-Defending Against the Social Networking Threat (OPSEC & SNS), Pre-deployment, Ombudsman, Family Readiness Group, Command Indoctrination, as well as tailored/specialized presentations. The OPSEC & SNS brief is by far the most requested and been presented to more than 40,000 military and family members over the past two years.

-- Computer-based training

Uncle Sam's OPSEC (USOPSEC) and OPSEC-Next Generation is located on Navy Knowledge Online (NKO) or provided on CD/DVD upon request. USOPSEC is the latest product and was featured in the Summer Edition of InfoDOMAIN.

-- Awareness products

Professionally produced short videos, many of which are currently aired overseas on Armed Forces Network; social networking, family, computer security at home, individual augmentee and identity theft brochures; plastic OPSEC reminder badges; posters; Plan of the Day/Week notices; social media handbook for ombudsman; sample Critical Information (CI) cue cards and CI lists.

-- Web Risk Assessment (WRA) support

The OPSEC WRA team conducts Web risk assessments on Navy Websites. Results are automatically forwarded to command's Web administrator.

-- One-stop shop websites and links on the unclassified site:

- **SharePoint** at https://www.portal.navy.mil/netwarcom/nioc-n/copcentral/opsec/default.aspx for references, products and calendar of events. Common Access Card (CAC) required.
- **Facebook** at http://www.facebook.com/navalopsec for the latest headlines and vulnerabilities on social networking and social media. The site is used to drive the OPSEC conversation and to make people aware of the latest and greatest changes in social networking.
- **YouTube** at http://www.youtube.com/navalopsec to view videos. Many of the NOST videos are located on YouTube as well as Facebook.
- **Slideshare** at http://www.slideshare.net/navalopsec for briefs. The briefs posted on slideshare are downloadable and "ready to use."

DOD and the recently signed Navy OPSEC instruction (OPNAVINST 3432.1A, 4 Aug 2011) direct commands to establish and utilize an OPSEC program, which is every command's first line of defense in combating adversarial intelligence collection against operations, missions, activities and Personal Identifying Information (PII). With the introduction and use of IbC, social networking and information sharing, practicing OPSEC is more critical now than it's ever been.

Contact any of the NOST members for additional information or assistance at opsec@navy.mil or by calling (757) 417-7100.

Herbert Relieves Meek as CYBERFOR Commander

From CYBERFOR Public Affairs

VIRGINIA BEACH, VA – RDML Gretchen S. Herbert relieved RADM Thomas P. Meek as commander, Navy Cyber Forces (CYBERFOR), in a ceremony June 22 at Joint Expeditionary Base Little Creek, Virginia Beach, VA.

"Cyber is at the backbone of everything we do every day," said Adm. John C. Harvey Jr., U.S. Fleet Forces commander, speaking to the CYBERFOR team at the ceremony. "The cyber threat is, as our president noted, one of the most serious economic and national security challenges we face as a nation. That is why your job is so important."

Meek assumed command of Navy Cyber Forces May 14, 2010. He is credited with establishing the Navy as a leader in cyber warfighting in the Department of Defense, and positioning the Navy to achieve Information Dominance during the coming decade.

"Our very existence as a command is due to the Navy's foresight to position our service as a leader in cyber," Meek said. "Navy instituted a more aggressive approach that harnesses the impressive talents of our cyber professionals and optimizes the cyber readiness of our afloat platforms and associated shore organizations. With the standup of a Cyber Fleet and Cyber TYCOM (Type Commander), and creating the Information Dominance Corps, the Navy affirmed its intentions and leadership in cyber capabilities and cyber warfare."

Commissioned through Aviation Officer Candidate School in 1982, Meek has served in intelligence, attaché, staff and community management positions. He is the recipient of the National Intelligence Reform Medal.

Meek reported to the National Geospatial-Intelligence Agency, North Fort Belvoir, Springfield, VA, where he serves as director of Military Support.

Herbert most recently served at the Pentagon as director of the Communications, Networks and Chief Information Officer (CIO) Division, on the staff of the Deputy Chief of Naval Operations for Information Dominance. She holds Master's degrees in Systems Technology (Space Systems Operations) from the Naval Postgraduate School and in Military Studies from the Marine Corps Command and Staff College.

A native of Rochester, NY, Herbert earned her commission in 1984 through the Naval Reserve Officer Training Corps (NROTC) program at the University of Rochester.

Herbert said she felt extraordinarily privileged to lead the CYBERFOR team in facing the formidable challenges ahead.

"Our focus will be on ensuring delivery of relevant, consequential and value-added C5I (Command, Control, Communications, Computers, Combat Systems and Intelligence) capabilities to our Fleet," Herbert said. "We will measure our success by the development of a highly skilled, adaptable and capable workforce, and in equipping those professionals with reliable, sustainable and fully interoperable networks, systems, capabilities and processes.

"Understanding that the stakes have never been higher, we will ensure that our Sailors and civilians are ready to fight and win in the global cyber domain," she said.

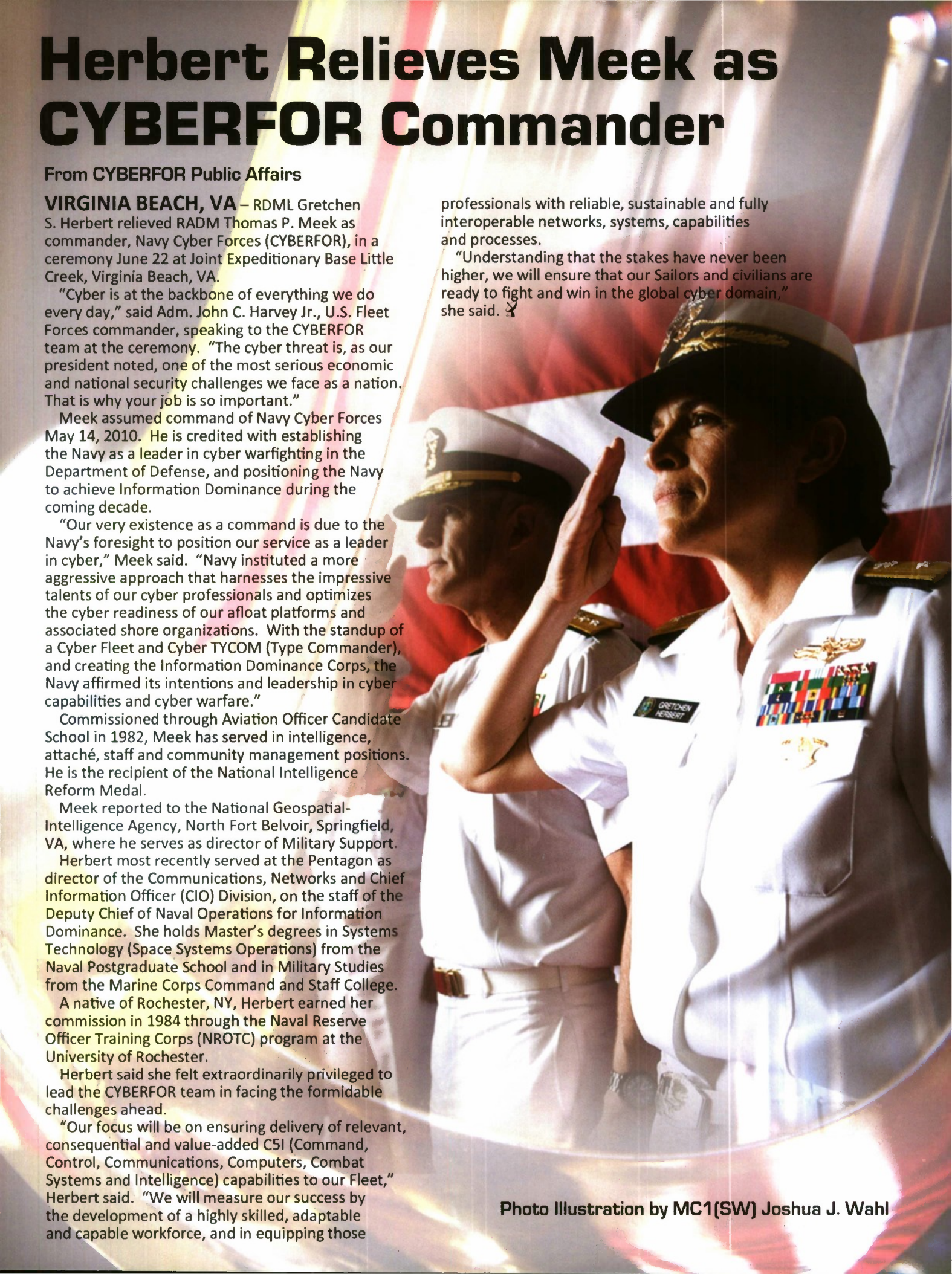


Photo Illustration by MC1(SW) Joshua J. Wahl

NETWARCOM Commander Retires

From NETWARCOM Public Affairs

VIRGINIA BEACH, VA – Naval Network Warfare Command (NETWARCOM) Commander, RADM Edward H. Deets, III, celebrated the culmination of a 32 year Navy career in a retirement ceremony at Joint Expeditionary Base, Little Creek - Fort Story, Aug. 5.

A native of Charlottesville, VA, Deets graduated from Duke University in 1979 where he was commissioned an ensign via the Naval Reserve Officer Training Corps.

During his career, he served on numerous ships; on the staff of the U.S. 6th Fleet in Gaeta, Italy; Korea and on the staff of Commander in Chief, U.S. Atlantic Fleet in Norfolk, VA.

After completing a tour as Commanding Officer of the Center for Cryptology, Corry Station, Pensacola, FL, he assumed duties as vice commander, NETWARCOM in 2005. He assumed command of NETWARCOM on May 14, 2010.

Citing the impact Deets had on the evolution of cyber in the Navy, VADM Barry McCullough, commander, U.S. Fleet Cyber Command and Commander, U.S. 10th Fleet, said, "your contribution to our way ahead cannot be overstated. It is the key to our success and will have a lasting effect on our warfighting capability for years to come. Your superior expertise and leadership supported the execution of national Navy policies in the development and implementation Information Warfare, Cryptologic, Network and Space Operations capabilities."

Deets recognized the many people who he worked with throughout his career and in the Information Dominance workforce.

"Serving this nation's most powerful fighting force, whether it's your first day or your last, it's all about living the dream – and I have been," Deets said. "The Navy has been my life and culture since reporting to Navy Reserve Officer Training at Duke University in 1975. Throughout my 32 years in the Navy, the duty stations and jobs changed, but the people didn't. It's the same passion for the work, the same strong leadership, and the same commitment. I am absolutely thrilled to have been part of Naval Network Warfare Command and to have had the opportunity to serve our great Navy and Nation.

A qualified Information Dominance Warfare Officer, Deets served as the leader of the Information Warfare and Cryptology Community. He attended the National War College at Fort McNair, Washington, DC, where he graduated with honors and received a Master of Science Degree in National Security Strategy with a concentration in Information Strategies.

Deets' personal awards include: the Navy Distinguished Service Medal, Legion of Merit, Defense Meritorious Service Medal, Meritorious Service Medal, Navy and Marine Corps Commendation Medal, Army Commendation Medal, and Navy and Marine Corps Achievement Medal.

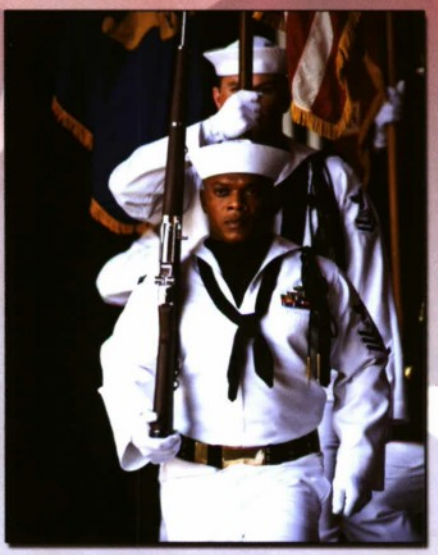


Photo Illustration by MC1(SW) Joshua J. Wahl

Photos by MC1(SW) Joshua J. Wahl & Robin D. Hicks

Learning to Operate in Cyberspace

With the establishment of U.S. Cyber Command and cyber security a national priority, operations in the 'fifth domain' are underway.

By RDML William E. Leigher, director of Warfare Integration (N2/N6F)

The term "cyberspace" designating a somewhat mystical and ever-evolving network of computers, routers, switches and people, emerged in fiction in William Gibson's 1982 novel Neuromancer. The definition usually cited from that work is "a consensual hallucination experienced daily by billions of legitimate operators . . . a graphic representation of data abstracted from banks of every computer in the human system . . . *unthinkable complexity* . . . lines of light ranged in the non-space of the mind, clusters and constellations of data" (emphasis added).[1]

The Department of Defense (DoD) defines cyberspace as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] Cyberspace operations is "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[3]

The DoD definition is meant to categorize doctrinally what is and what is not a cyber operation. But what does Gibson mean by operating in cyberspace's " unthinkable complexity"?

The Reality behind the Words

Definitions continue to evolve. But the real work ahead is describing the model for operating in cyberspace in a way that is analogous to a description of operating in the maritime or air domains. Cyberspace is a domain, and the Navy needs to approach it as such. The relationship of cyber activities to those in the domains of sea, land, air and space also must be defined. No domain stands on its own.

About four years ago, the declaration of cyberspace as the fifth domain did not come without pushback. The argument generally goes that sea, land, air and space emerge from nature, but cyberspace is completely man-made. While this is true, one logical model is analogous to the thinking about and using cyberspace as an operational domain.

Dan Keuhl from the National Defense University developed a model that suggests networks, and the attached devices and software that we use, make cyberspace relevant in a military sense.[4] Counterparts in the other domains would be vehicles, ships, airplanes and satellites. Operating in and exploiting cyberspace can be seen as parallel to operating in the other domains, in the sense that each has unique physical characteristics. In this way, cyberspace is physically just as real as the other four domains.

How the Navy Operates

After we accept cyberspace as a domain, our thought process can shift to what it means to operate there. Specific warfighting principles must be developed – though what we understand about operations in the maritime and air domains has general analogies in cyberspace. The current methods of operating in cyberspace are not serving the Navy as well as they should be. In fact, principles currently in practice would not be tolerated in any other warfighting domain. Here are some examples:

- In the 1990s, the Navy created the Navy Computer Task Force – Computer Network Defense (NCTFCND), in response to intrusions into our unclassified networks. This command evolved into the Naval Computer Incident Response Team, and eventually the Navy Cyber Defense Operations Command (NCDOC). Throughout this evolution, sensors were deployed to better detect intrusion – and, while the sensors themselves evolved, the operational mindset has remained on forensic study of malware and patching. We have not developed our way of thinking to grasp an active defense against external threats that will both prevent penetration and neutralize threats discovered inside our networks.

  This has led to an ever-stronger fortification of our networks, but it has not resulted in better defenses. Unauthorized users continue to penetrate networks, and ways in which we can use networks to our benefit are increasingly restricted.
- Current Computer Network Defense (CND) practice is fundamentally reactive, not the predictive system used in the other operational domains. A reactive system is signature-based, meaning it only recognizes malware that has been detected previously, and does not provide warning for new software or exploits used to penetrate networks. This sort of operational methodology worked for antiship missile defense and electronic warfare, because the radars that missiles use to obtain a final targeting solution were not easily reprogrammable. This approach fails in an

information-age environment where software can be altered in minutes to completely change the nature of a threat.

- Networks are not operated with the same rigor as systems critical to other warfare disciplines. In a manner consistent with our network – defense philosophy, the Navy has deployed sensors to better understand how our data flow and bandwidth are used. Software has been customized to allow the Navy's network operating centers to monitor in real time the performance of individual nodes for a strike group or theater. Yet we do not routinely operate this way in support of the numbered Fleet commands' communications and networking. This is analogous to radiating radar while having the repeaters throughout the ship switched off.

Life on the Network

Successfully operating in cyberspace will involve adopting a model significantly different from current practices. The U.S. Tenth Fleet is rapidly developing and implementing a philosophy that supports real-time network operations and defense. It is based on three principles:

- Assure that Command and Control (C2) is in place so forces can be used.
- Maintain freedom of maneuver in cyberspace to allow the Navy to fight in the manner desired.
- Provide non-kinetic effects, or military fires that do not depend on explosives, to achieve a desired outcome – offensive and defensive – in support of joint and Navy commanders.

These three lines of operation are both parallel and sequential. The continuum between operating and defending networks begins with the requirement to provide assured, continuous C2 and extends to ensuring that the Navy can use cyberspace to its advantage. The adjacent range of operations involving exploitation and attacks in cyberspace makes use of the same freedom of navigation to move freely between protected operating areas and foreign cyberspace.

A key to operational success will be developing a workforce with the skills to 'live' on the network. Our cyberspace operators must continually train and execute in the operating environment. In the same way, a submarine gains tactical advantage from operating in the subsurface environment while concurrently countering adversaries.

In cyberspace, this means developing defensive and offensive cyber-warfighting skills through 'on-net' operator proficiency. The network has a character and flow that can be compared to the effects of weather or terrain in maritime and land domains. This sense of the domain has a direct relationship with tactics and the delivery of material in support of a campaign. Navy tactics, techniques and procedures will evolve rapidly as Sailors gain operational-domain experience.

Defensive Actions

During peacetime and in phases 0, 1 and 2 of conflict, we are very comfortable thinking through the defensive aspects of warfare. Most of anti-air warfare is defensive in nature in that it protects high-value units, and much of the contemporary discussion about maritime and air domain is dominated by ballistic-missile defense. The same is generally true of antisubmarine warfare and a discussion of barriers and choke points. Thus, it is natural that defensive measures figure prominently in the cyberspace warfighting discussion.

The first step is to develop a strategy and set of operational practices to defend cyberspace as an operational domain. As for most such procedures, rules of thumb guide network defense. First is the 85 percent rule, referring to the percentage of problems normally confronting the Navy that basic network security can handle. This includes a modern operating system that is regularly patched with strong passwords and sound training. Programmatic solutions primarily satisfy these responsibilities through servicing, manning, training and equipping.

It is not unlike preparing for damage control. The remaining 15 percent of the problem is the dynamic part of network defense in which we confront adversaries and actors who, for varying reasons, attempt to penetrate Navy networks.

Aggressive Tactics

The tactics applied to the 15 percent solution include service and national sensors that are used to knock down known threats. This is the operational role of the network defense service providers such as NCDOC. But there are shortfalls to a sensor and/or signature-based system. As noted earlier, these capabilities have been deployed reactively instead of in a predictive way.

Even as we learn to use sensors in a real-time manner, operationally these systems have a significant shortcoming. Like the SLQ-32 Electronic Warfare system, they hit only on known radar signatures. This means that a network exploit not yet discovered is unlikely to be detected.

Changes to the cyber environment may happen instantaneously, so the sensor-based systems must operate at network speed, with operators monitoring but not executing individual actions. Though the stealth-like features and speed of the engagement in cyberspace are operationally challenging, the difficulty in attributing an attack to a specific entity may be a show-stopper with rules of engagement. Actions taken by a nation-state versus patriotic hackers acting on behalf of a nation are easily blurred. This was the likely scenario in the brief 2008 conflict between Russia and Georgia. It is not always evident against whom network defenders are protecting. The right of self-defense in cyberspace has not been thoroughly established. Most discussion of defensive cyberspace actions focuses on CND-Response Actions (CND-RA) and not denying operating space to an adversary.

. . . continued on Page 30

Doctrinally, CND-RA is the ability to remotely 'hack back' to an attacker or intruder who has penetrated a network or computer system. The reasonable analogy in the other domains is a counter-fire strike, which is an offensive tactic to deny an adversary further action. Developing the capability to conduct CND-RA is important, but it is secondary to protecting the network as an operational environment and denying that space to an adversary.

To actively defend, network operators must be able to see and understand how our own systems work and how information flows through them, as well as visualizing the impact of external forces attempting to penetrate friendly cyber environments. The real-time awareness of cyberspace and experienced operators with on-net skills will become the basis for dynamic network-defense operations and the principal element in protecting cyberspace as an operational environment.

Going on Offense

We must learn how to select targets in cyberspace. As in the other warfighting domains, the choice and tactical employment of weapons makes a difference. With physical targets, the range of the delivery platform or a weapon system is a limiting factor in the ability to strike. The factors considered by a cyber-attack planner are different from those faced by a kinetic weaponeer.

In cyberspace, access to a specific target at a particular time may depend on the on-net operator's ability to understand and react to changes to networks or operating systems in an environment that contains both hardware and software components. Early attempts to select cyber targets have concentrated on developing methods to use network attack as a way to neutralize targets that defy a kinetic solution.

While cyber-attack planners certainly must work to develop capabilities against hard targets, the offensive use of cyberspace will probably evolve in a much more measured way. Options to use denial-of-service weapons or controlling botnets (robot networks that operate autonomously) to limit an adversary's ability to use cyberspace are the likely first offensive tactics. In terms of effect on the campaign, these can be considered 'level of effort' targets to degrade an adversary's C2 or disrupt the left side of the kill chain, or those intelligence and targeting activities that provide the firing solution.

In the near future, efforts may be focused on integrating a campaign that supports actions in phase 2 of the conflict. However, because cyber weapons are nondestructive and may be unattributable, consideration must be given to their use during phases 0 and 1 of conflict to shape impending hostilities and provide alternatives to destructive weapons at later stages in the confrontation. Cyber-attack planners will also consider delivering 'effects', or various types of malware, to opponents as a de-escalatory measure.

Both the longevity of the effect delivered and second- and third-order effects are also offensive cyberspace considerations. In the near term, sequencing of an attack in conjunction with kinetic strikes and the persistency of effects will be the focus of cyber planning.

A next step in the evolution of offensive cyberspace may be the delivery of effects to shape a campaign or to seize the initiative in attacking a specific target. This may degrade a specific capability that is key to the center of gravity, such as logistics. It may also focus on targets outside the geographic area of operations to either distract a defender from the main efforts or target a national-level capability such as public utilities or financial systems.

As cyber targeteering matures, additional factors such as the integration of cyber effects throughout a campaign, added emphasis on precision attacks on military targets, and controlling unintended consequences like damage to innocent cyberspace 'bystanders' will be added to a planner's considerations

Experience with kinetic strikes has led to 'no-strike' lists or other sets of rules that help control engagements. Because of the interdependencies of networks and systems, cyberspace presents its own challenges. Attacking a control system for a power grid may provide the commander options to disable defensive systems, but cascading effects from the loss of electrical power to a region must also be considered. This is not a unique problem, but it is one with which cyber planners have little practical experience.

Command and Control and Cyberspace

Philosophically, challenges include making the distinction between cyberspace as an operational domain and the systems that constitute the capabilities of cyberspace. Early doctrinal discussion led to coining the term C5I - Command, Control, Communications, Computers, Combat systems and Intelligence.

It was seen as a set of operational and tactical-level processes, decision aids and awareness or visualization tools. But the C5I discussion falls far short of helping guide our way through cyberspace operations, particularly because C2 is a command function that draws from each warfighting domain. Cyberspace has its own operational characteristics and tactics, techniques, and procedures, as well as a specific relationship with the principles of C2 and the 17 elements of operational art.

Command being the inherent responsibility for the commander, the question becomes controlling cyberspace operations. In this regard, it is instructive to review ADM Robert Willard's seminal article "Rediscover the Art of Command and Control" (U.S. Naval Institute Proceedings, October 2002). Willard's basic rule of effective C2 requires that the commander exercising control should have "better insight into what is required to win the day than is evidenced by the subordinate commander's actions."[5] Thus, the question of the commander's ability to 'control' in cyberspace guides not only what happens in cyberspace, but also the actions that must be synchronized with operations in the other domains.

Following are the commander's objectives for exerting control, implying the task of synchronization between various warfare areas and operational functions.

- Maintain alignment with the operational mission.
- Provide situational awareness in the framework of the agreed-upon common operational picture.
- Advance the plan on the timeline and adjust to deviations accordingly.

- Comply with procedure to achieve standardization and effectiveness.
- Counter the enemy and be responsive to emerging intelligence, surveillance and reconnaissance.
- Adjust apportionment of assets and resources, including time.[6]

Each of these six objectives applies to cyberspace operations. Although the latter share some characterizations with other domains, their most common feature is time – specifically, speed of execution. This becomes clear through a comparison with antisubmarine warfare. As in cyberspace, submariners are challenged to operate in the same environment as does an adversary submarine. However, whereas antisubmarine warfare develops relatively slowly, cyber operations can change significantly in milliseconds. As cyberspace tactics, techniques and procedures evolve, it will be critical to understand both the unique and the similar aspects of control functions.

A Model for Cyber C2

In May 2010, the U.S. 10th Fleet staff, along with several partner commands and corporations, deployed in support of U.S. Pacific Command and Commander, Joint Task Force (CJTF)-519, to participate in Exercise Terminal Fury 2010 (TF10). Operating as the Joint Cyber Operations Task Force, the staff used a prototype organizational model to test cyberspace operational principles and exercise command and control of assigned forces.

Approximately 150 personnel supported the task force at various locations in Pacific Command. A facility was created to assess emerging cyberspace control concepts and provide a planning location for specific defensive and offensive effects. The main cell included industry partners who used specific cyberspace visualization and analysis techniques.

The Joint Cyber Operations Task Force is an emerging concept that will continue to develop. In the context of Navy and DoD organization, the exercise was conducted during a period of significant organizational change for cyber forces. U.S. 10th Fleet had been in commission for less than five months, and U.S. Cyber Command had its formal establishment ceremony while TF10, and cyberspace exercises had not been extensively planned. The operational design allowed the task force commander to exercise authorities held by U.S. Cyber Command, as well as being operationally responsive to both the Pacific Command and CJTF-519 commanders.

The Pacific-based commanders used the model effectively, and it received positive feedback as an organizational structure for cyber C2. Additional exercises must be conducted to more thoroughly integrate the Joint Cyber Operations Task Force structure with established Intelligence (J2), Operations (J3), and Command, Control, Communications and Computer Systems (J6) organizations of the combatant commands. Sound doctrine to support the operational level of war for cyberspace operations is needed, similar to the principles of maneuver. From the doctrine and tactics, commanders will better understand cyber operations, especially as they relate to those in the other domains

As Willard stated, the "tenets of C2 are timeless, but with cyber operations, warfare is faster and more complex, thus commanders must assimilate the six areas of control at high speed and in conjunction with other warfare area plans."[7] Although the speed of cyberspace activity is a distinctive feature of the domain, TF10 put it in the context of a major theater operation and demonstrated that adapting operational principles from other warfare areas can work in cyberspace

The experience also showed the need to align cyber operations with service components and combatant commanders. Although the latter have the requirement to completely understand all aspects of an operation, execution is the responsibility of the service components. Because joint-force maritime and air-component commanders' execution depends on sound network operations and defense, the services must retain C2 of these functions without impeding the combatant commander's responsibility to move the plan forward

The Navy's network, intelligence and leadership were organized during the past year to maintain the service as the finest in the world. Just as air power developed rapidly at the onset of World War II, cyberspace operations will proceed apace, given the existing threats and opportunities. The seams in cyber C2 will be closed with exercises and experiences.

As our understanding and visualization of it improves, cyberspace's relationship to and synchronization with the other domains will guide the way to new defensive and offensive capabilities, increasing the combat effect for both cyber and kinetic weapons. Time is of the essence. U.S. 10th Fleet and its partners will rapidly engineer and field new operational capabilities to take full advantage of cyberspace.

1. William Gibson, Neuromancer (New York: Ace, 1984), p. 268.

2. Joint Pub 1 Doctrine for the Armed Forces of the United States (Washington, DC: Joint Staff), dated May 2, 2007 and incorporating change 1, March 20, 2009) GL-8.

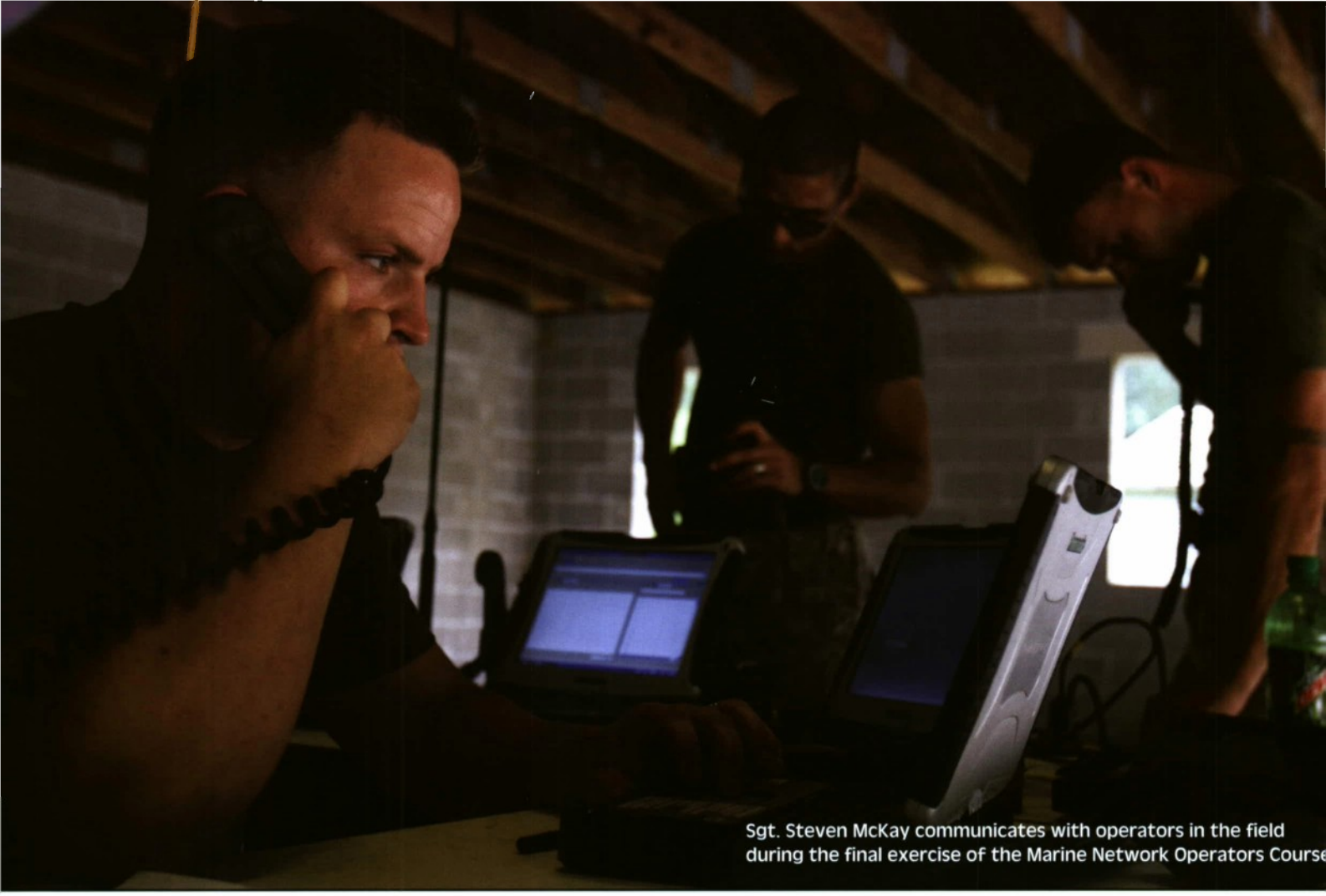
3. Joint Pub 1-02, DOD dictionary of Military and Related Terms (Washington, DC: Joint Staff), dated April 12, 2001 and amended through September 30, 2010, p. 118.

4. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," Cyberpower and National Security, ed. Franklin D. Kramer, et al. (Dulles, VA: National Defense University Press and Potomac Books 2009), p. 29.

5. Robert F. Willard, "Rediscover the Art of Command and Control," U.S. Naval Institute Proceedings, October 2002, p. 53.

6. Ibid., 53–54.

7. Ibid., 54.



Sgt. Steven McKay communicates with operators in the field during the final exercise of the Marine Network Operators Course

U.S. Marines Creating Island for Network Defense

TOP INFORMATION TECHNOLOGY OFFICER TACKLES NETWORK CHALLENGES FOR THE CORPS

By George I. Seffers, SIGNAL Magazine March 2011

The head information technology officer for the U.S. Marine Corps, Brig. Gen. Kevin Nally, is grappling with several projects necessary to keep critical information flowing smoothly and securely. Nally's efforts include dramatically streamlining a sprawling information technology infrastructure, overseeing the Defense Department's information assurance range, protecting information in the era of social networks and WikiLeaks and transitioning from the Navy-Marine Corps Intranet (NMCI) to the Next Generation Enterprise Network (NGEN).

The general, who took over his current responsibilities in November, is the Marine Corps director of Command, Control, Communications and Computers (C4), the Navy's deputy chief information officer for the Marine Corps, and the deputy commander for Marine Corps Cyber Command, but he is commonly referred to as the Marine chief information officer. He officially donned the multiple hats on Nov. 10, the Corps' 235th birthday.

Among the projects on his to-do list, Nally will help streamline the Marine Corps' expansive information technology infrastructure into a tightly integrated, agile, defensible and survivable network capable of supporting distributed battlefield operations as well as an efficient and effective business enterprise. Plans call for a major data center located in Kansas City, MO, to be complemented by four regional network operations and security centers and eight information technology support centers.

"What we're creating is an island of defense, so you may be able to cut off part of the network from a cyber attack, but you won't be able to cut off the entire network," Nally said.

The Marine Corps Enterprise Information Technology Services data center in Kansas City will support the data processing requirements for the entire Marine Corps. It will provide application hosting capabilities,

enterprise shared services, access to enterprise wide information and collaboration and information sharing across business and warfighter domains. It is designed to deliver an infrastructure that can adapt readily to evolving requirements for software, hardware, data, services and management. The center will clear initial operational capability this summer, according to Nally, and it will offer several benefits, including program consolidation, efficiency and continuity of operations.

In addition to the Kansas City data center, the Corps' streamlined architecture will include four regional network operations and security centers and just eight Marine Air-Ground Task Force (MAGTF) Information Technology Support Centers (MITSCs), which constitutes a dramatic reduction.

"We're going from 40 MAGTF support centers to just eight, and they're going to be regionalized. We'll also have four network operational support centers. It's going to increase our effectiveness in supporting the warfighters and will make us more efficient and reduce costs," Nally said.

The Marines announced in October the opening of a new MITSC at Camp Pendleton, CA. The center is known as MITSC West, and it includes a customer support center, network operations facility and multiple status screens with real-time displays monitoring network health. It is designed to foster a proactive approach to network maintenance and responsive customer service. It will serve seven installations in Southern California and Arizona as well as the Marine Corps Recruit Depot in San Diego. MITSC West is designed to support the transition from NMCI to NGEN, the first step toward achieving the Navy's vision of a future fully integrated Naval Networking Environment (NNE). That transition is another of Nally's top priorities. The Navy has awarded a contract to Hewlett-Packard to continue services provided under NMCI, which serves more than 700,000 personnel, until the transition to NGEN is complete. The Marines, however, have wasted no time beginning the transition from the commercially operated network to the Defense Department network. The intent is to move more than 1,200 users by the end of this month, which Nally predicts will be no problem because in January they began using an automated system for moving personnel, rather than doing it manually.

"My guess is we'll be done well before March 31st," he said.

Nally says one of the biggest advantages over NMCI is that NGEN will be government-owned and operated, giving Marines greater control.

"The most important thing to me is that we're going to be able to meet the commander's requirements in a more timely manner because we're going to be able to set the priorities in terms of taskings," he said. "In the past, the tasking priorities may not have been what the commander really needed, so we as the Marines will be able say what today's priorities are."

Rather than one large contract with one vendor, the Navy intends to award five separate contracts—for transport services, end-user hardware, enterprise software licensing, enterprise licensing and independent security operations oversight and assessment—but the Marines are opting out of the security operations segment of the contract.

"The four we're looking at are transport, hardware, software and the enterprise service model. The Navy's also looking at information security operations, but that's the one out of the five that we're not going to participate in because we operate our own network and we don't want to contract that out," said Nally.

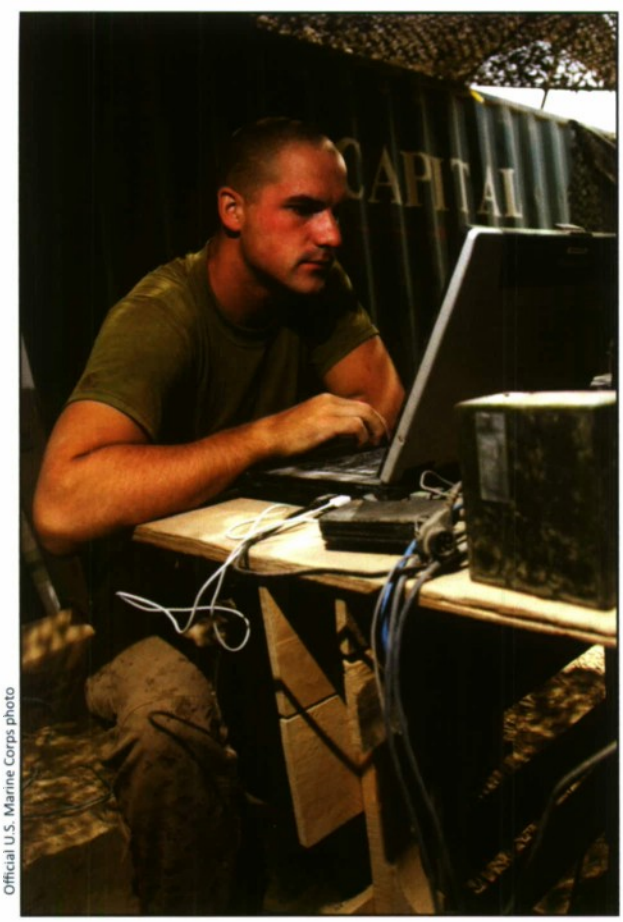
On another network security front, Nally reveals that the Marines recently have been named by the Defense Department as the executive agent for the Information Assurance Range. Not to be confused with the Defense Advanced Research Projects Agency's National Cyber Range research and development program, the current Information Assurance Range offers a closed, Internet-type environment for joint cyber exercises. It includes both malicious and benign websites and can be used for testing information assurance products and for training personnel at all levels. The Marines are working closely with the Defense Information Systems Agency on the project.

"We'll use it as a training and education tool for the information assurance work force, to include cyber forces. We'll ensure that information assurance is inherent to the system, thus providing superior and transparent threat protection for a wide range of missions," Nally said. "We'll be able to test and evaluate

. . . continued on Page 34

"What we're creating is an island of defense, so you may be able to cut off part of the network from a cyber attack, but you won't be able to cut off the entire network."

- Brig. Gen. Kevin Nally, USMC, director of Command, Control, Communications and Computers (C4) and the Navy's deputy chief information officer for the Marine Corps and the deputy commander for Marine Corps Cyber Command.



Official U.S. Marine Corps photo

new software products and learn how to look for, find and finish malicious software."

The general's office also helped coordinate the recent deployment of the Host Based Security System to Marine Corps units in Afghanistan. The system is a commercial product that prevents, monitors, detects, tracks, reports and counters known cyber threats to Defense Department networks. It is to be attached to each of the department's host servers and will be managed by local network administrators and configured to address known exploits using an intrusion prevention system and host firewall.

Also in the information assurance realm, the Marines continue to refine their approach to social networking sites and other websites such as WikiLeaks. Nally discloses that the Marines have an informal agreement with Facebook to remove any pages that violate operational security, reveal personally identifiable information on Marine Corps personnel or impersonate Marine Corps personnel for the purpose of scamming innocent users. The Marine Corps public affairs office monitors Facebook and can, if need be, contact Facebook staff to have a site removed. The Marines have held discussions with other social networking sites, but have not yet reached agreements with them.

"We've partnered with Facebook so that if there are any operational security incidents that go on a Facebook account, we can contact Facebook headquarters, and they will pull that site immediately," Nally said. "Social networking sites provide a morale value for our force, and it's a great way for our forces to pass information back to their loved ones, but we also possess certain vulnerabilities that they need to be aware of—especially when it comes to operational security and personally identifiable information concerns."

The Marines also struggle to keep Corps computers disconnected from WikiLeaks, the infamous website that has leaked reams of classified data. WikiLeaks has been blocked from the Secret Internet Protocol Router Network, or SIPRNet, but keeping it blocked remains a challenge.

Official U.S. Marine Corps photo

"We're taking appropriate steps to deny access to it. Most of that guidance comes from components of U.S. Cyber Command and then we draft policies to implement, but they move those WikiLeaks sites from one Internet service provider site to another or change the name," Nally said. "The challenge is going out and finding the new site and blocking that as well, but we're proactively doing that."

The array of projects and issues he deals with fit into the overall vision for a "knowledge-based force that leverages seamless enterprise capabilities across the spectrum of conflict in order to enhance decision making, achieve knowledge superiority, and gain tactical, operational, and strategic advantage over our nation's adversaries."

The knowledge-based force is more than a catch phrase for Nally — it is an imperative.

"Knowledge is a strategic force enabler. The goal is to have a seamless enterprise capability to enhance decision making — to turn information into knowledge so that it's in the right format and usable," Nally said.

He lists his top priorities as the work force — including Marines, civilians, contractors and especially the warfighters; the continuity of services contract and NGEN; support to MAGTFs and the supporting establishment; amphibious C4; chief information office governance and processes; science and technology; information assurance; cyber; and C4 information management and C4 strategic communications plan. For the work force, he emphasizes the continuing need for training and educating the work force and raising awareness of information assurance issues because, as Nally said, "The best network security is a well-trained Marine," to improve the production, distribution and application of precise time.

1. The Navy is investing in upgrades to the USNO Master Clock to meet the latest DoD requirements. A set of new atomic rubidium fountain clocks is being built and tested by USNO scientists. These clocks are on track to enter operations in 2013 and will improve Master Clock precision by a factor of 100 in order to meet the higher time and positioning accuracy requirements for GPS-III system.

2. USNO is working with the Defense Information Security Agency (DISA) to develop an authentication process for Network Time Protocol time (NTP) distribution over NIPRNET and SIPRNET. In order to provide coordinated network timing, Joint Task Force for Global Network

Operations has already directed DoD users to use USNO servers as the NTP source. USNO's efforts with DISA to establish authentication processes will improve security and help ensure authoritative time distribution on DoD networks.

3. The current primary navigation and time source on major combatants is the Navigation Sensor System Interface (NAVSSI) system. NAVSSI provides positioning and time information for the all internal weapon, combat, command and control and communication systems throughout the ship. NAVSSI uses UTC (USNO) time, received from GPS, and has an internal rubidium oscillator able to maintain an accuracy of 0.1 to 1.0 microseconds for up to three and a half days if the GPS signal is lost. The NAVSSI design integrates anti-jam GPS antennas and other shipboard navigation sensors to provide a highly redundant capability.

4. The next generation shipboard positioning and time distribution system is GPNTS (GPS-based PNT Service). GPNTS will enter the fleet in FY16 and provides a number of capabilities designed to increase time and positioning integrity for operations in GPS-challenged environments.

TEAM SPAWAR

CANES Program Successfully Achieves Critical Design Review

By Steven A. Davis, SPAWAR Public Affairs Office

SAN DIEGO - The Consolidated Afloat Networks and Enterprise Services (CANES) program recently achieved a significant engineering milestone with the completion of Critical Design Reviews (CDR) for the two competing CANES systems being developed by Lockheed Martin Mission Systems and Sensors and Northrop Grumman Information Systems.

"CDR is a key point in the CANES program as it establishes the design baseline and provides assurances that CANES will meet stated performance requirements within cost and schedule parameters," said CAPT D.J. LeGoff, program manager for the Tactical Networks Program Office. "We are confidently proceeding into system fabrication, demonstration and test."

The next step in the Engineering and Manufacturing Development (EMD) phase of the program is completion of a Test Readiness Review. This review will ensure that the CANES design is ready to proceed into formal Contractor System Integration Test prior to down-select to a single CANES design. The review will also assess test objectives, test methods and procedures, and scope of testing while verifying the traceability of testing to program requirements.

The CANES program has recently re-structured its programmatic schedule as a result of the fiscal year 2011 budget approval delays. The EMD phase of the contract was delayed five months, but all major acquisition milestones are still achievable within approved parameters and the first CANES installation on a fleet destroyer is planned for late in fiscal year 2012.

CANES is one of several Acquisition Category I programs in the Program Executive Office, Command, Control, Communications and Intelligence (PEO C4I) portfolio. CANES represents the consolidation and enhancement of five shipboard legacy network programs to provide the common computing environment infrastructure for command, control, intelligence and logistics applications.

Consolidation through CANES will eliminate many legacy, stand-alone networks while providing an adaptable and responsive information technology platform to rapidly meet changing warfighter requirements. This strategy strengthens the network's infrastructure, improves security, reduces the existing hardware footprint and decreases total ownership costs. In addition to providing greater capability, CANES will allow Sailors to benefit from reduced operations and sustainment workloads as a result of common equipment, training and logistics.

About SPAWAR

As the Navy's Information Dominance systems command, SPAWAR designs, develops and deploys advanced communications and information capabilities. With more than 8,900 active duty military and civil service professionals located around the world and close to the fleet, SPAWAR is at the forefront of research, engineering, acquisition and support services that provide vital decision superiority to our forces at the right time and for the right cost.

NOTE: Further CANES materials can be found at the PEO C4I website:
www.public.navy.mil/spawar/PEOC4I/Press/Pages/default.aspx

JOINT IO RANGE – "CYBER" RANGE IN A BOX

By Jacky Fisher, CYBERFOR Public Affairs

Previous InfoDOMAIN issues gave readers an inside look at those who train on the U.S. Joint Forces Command (JFCOM) Joint Information Operations (IO) Range and the administrative requirements required to train. On Aug. 4, JFCOM was disestablished and the Joint IO Range was realigned under the Joint Staff - J7, Joint Coalition Warfighting in Suffolk, VA. This edition concludes the series with the "nuts and bolts" of cyber training, its scope and an idea of what an event may encompass.

U.S. Joint Forces Command (JFCOM) has provided a training venue that's been used by all branches of the U.S. military, several U.S. Combatant Commanders (COCOMS), and many Department of Defense (DOD) agencies that is without walls, is sometimes on wheels, and can be global, even stratospheric, in scope.

The Joint Information Operation (IO) Range, now realigned under the Joint Staff - J7 since the recent disestablishment of JFCOM, is where those engaged in non-kinetic warfare can exercise IO weapons and capabilities. The Joint IO Range provides this transportable venue with IO Range Service Delivery Point version 2.0 (SDP v2.0) equipment suites.

This lightweight, portable, *cyber* range in a box is a key component for testing IO weapons, systems and capabilities. Figure 1, Joint IO Range Alliance, illustrates the breadth of the Joint IO Range venue. The SDP's versatility allows the Joint IO Range to host a single exercise or several events concurrently.

Managed by the Joint IO Range Operations Center, SDPs create multiple Virtual Private Networks (VPNs) that can host numerous exercises simultaneously. VPNs allows each exercise to be conducted in its own 'cloud', keeping classified traffic within its individual properly classified pipeline, separated from other scenarios' traffic as well as real-world traffic.

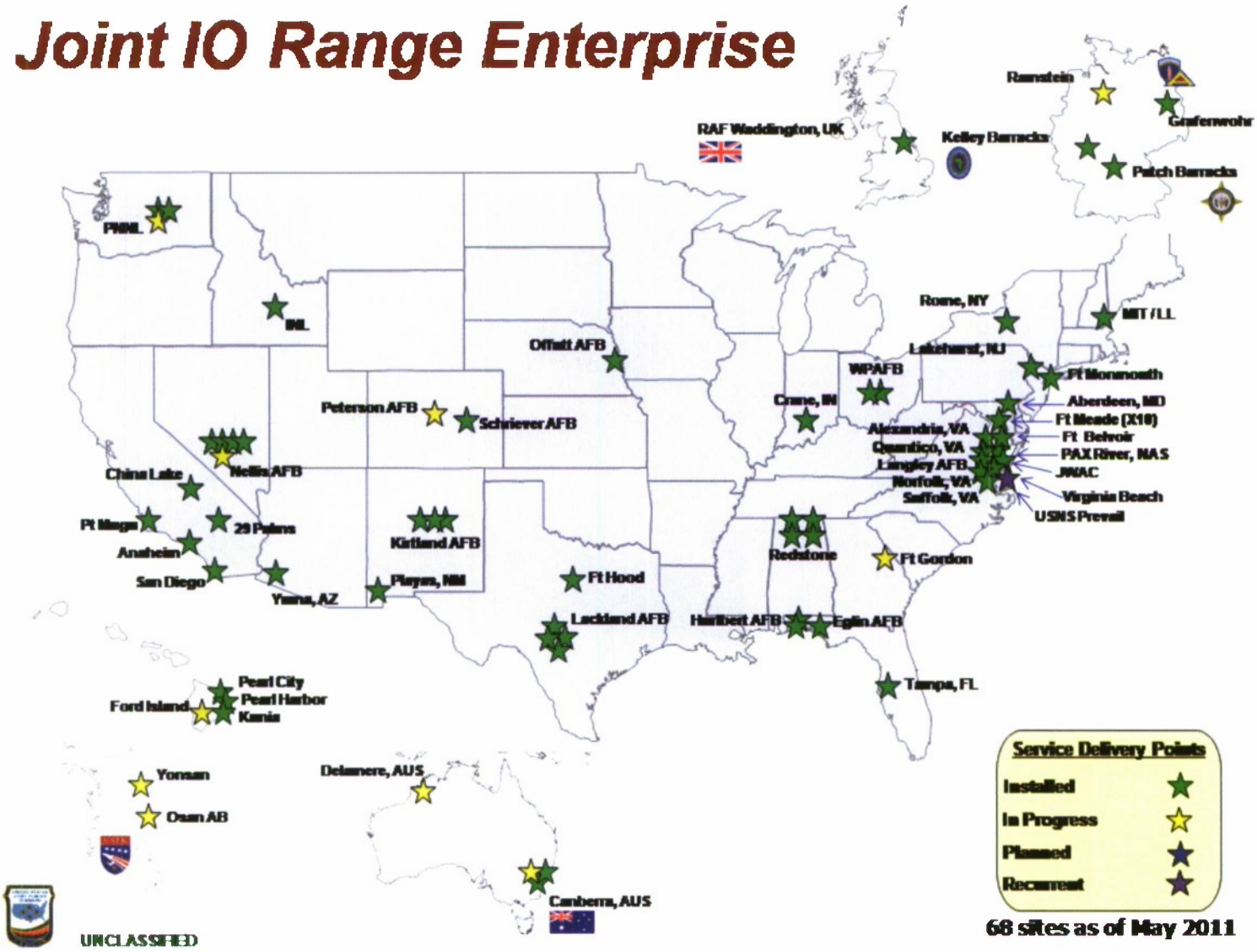
"The versatility coupled with the capability of the SDP creates a virtual environment that allows cyber exercises to be conducted securely," said Chuck Campbell, deputy chief of the Joint IO Range, referring to the PL3 (Protection Level-3) designation granted in 2007 by the Special Category Information System (see InfoDOMAIN Summer 2011 Edition, Joint IO Range story). "The SDP provides a persistent connectivity between all Joint IO Range sites while segregating and isolating user communities to mitigate the risk of co-mingling multiple classification levels."

"The Joint IO Range operates in a parallel universe of sorts," said Campbell. "That's the reason that capabilities like the Joint IO Range were created. It doesn't plug in to the SIPRNET, JWICS or the NIPRNET (real-world networks for classified and unclassified traffic). There is no risk to bringing these systems to their knees or compromising them."

Because of the PL3 designation and the closed loop network environment, a system does not have to be accredited to participate on the Joint IO Range.

"When we set up an event with a customer ... everyone agrees what various devices are going to be connected to which VPN, for how long, and in what manner," said Army Lt. Col. John Ballard, chief, Joint IO Range. "That is what governs the connection. This

Joint IO Range Enterprise



is what my technical staff spends 99 percent of its time doing, and then implementing it (the exercise) once the agreement is signed."

With numerous events concurrently but independently running, the Joint IO Range can theoretically create time -- get more than a traditional 40 hour work week from hosting multiple exercises. In fiscal year 2010, the Joint IO Range exercised more than 131,600 hours, hosting 65 events. SDPs are capable of hosting multiple events simultaneously, which allows several customers to utilize the same capability many times over without overlapping into another's event.

"It's much like the golf driving ranges," said Ballard. "They're stacked several levels high to allow many people to use that one capability many times over simultaneously. Events are run via SDPs with the same concept in mind."

The cyber range gives warfighters the capability of assessing both kinetic and non-kinetic effects in the battlespace, inside an enemy's decision cycle. "We now have the ability to test, train and live fire in a controlled environment," said Ballard. "The cyber range creates an environment without the limitations of operating on a 'live' network, allowing warfighters to explore the 'art of the possible'."

For more information on how your command can use the Joint IO Range, contact the Joint IO Range requirements lead Dave Blake, Joint IO Range Requirements, at IOR-Reqs@hr.js.mil or david.blake.ctr@hr.js.mil, (757) 836-9651. Reserve Units or reserve personnel with security clearances wanting to drill at one of the Joint IO Range sites, contact Chuck Campbell, chuck.campbell@hr.js.mil, (757) 836-9948.

DoD Names NCTAMS LANT's DEFY Program Number One ... Again

From CYBERFOR Public Affairs

The Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT) Drug Education for Youth (DEFY) Program has been selected as the best drug awareness and outreach program in the Navy for the second time in three years.

NCTAMS LANT was also named best Navy DEFY program in 2008.

"This award would not be possible without the dedicated military and civilian volunteers who take two weeks off from work each summer, and one Saturday a month for 10 months, to mentor boys and girls," said Sharon Shaw, CYBERFOR administrative/protocol officer. Shaw formerly worked at NCTAMS LANT, and has coordinated the command's DEFY program for 11 years.

DEFY is designed to address problems faced by today's youth, including violence, drug use and dropping out of school, which may minimize opportunities for success for young people.

Volunteers ITSN Edward Hegwood (left) YN1 Michael HighTower (center) and IT3 Melissa Johnson (right) participate in a DEFY class. (Official U.S. Navy Photo)

"We teach the kids various lessons to include drug education, gang resistance, police and fire safety, nutrition, study habits and cultural differences," said Shaw.

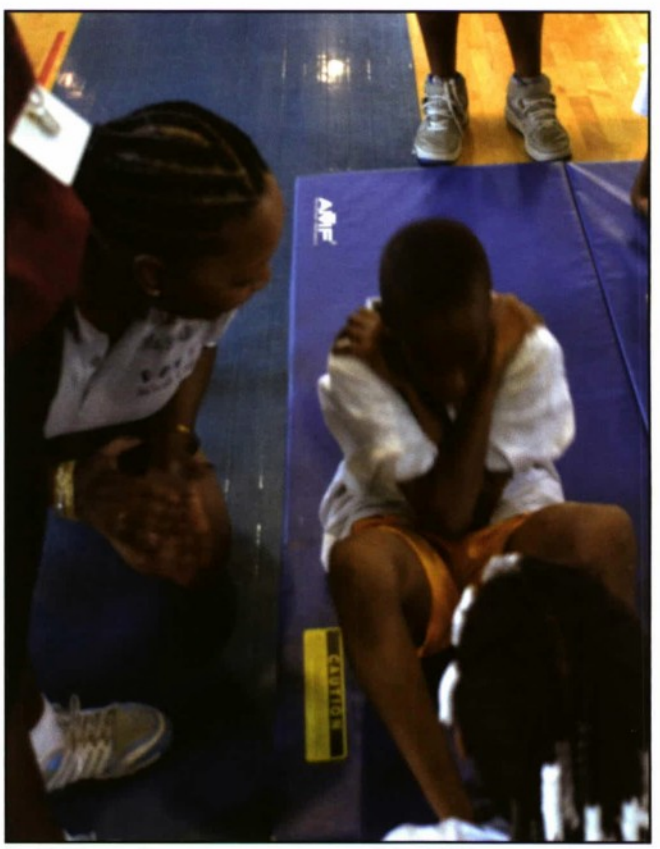
The DEFY program helps reinforce positive values, teaches important life skills and equips young people to resist alcohol and other drugs. The program provides opportunities for kids to learn about themselves, their peers and how to make positive choices that will help them succeed.

"DEFY is a great program that both effects our DoD and military children by providing positive feedback," said NCC (IDW/SW/AW) Anthony Darby, NCTAMS LANT Career Counselor and DEFY program assistant coordinator. "Many of our mentors bring first-hand knowledge and experience to our program, which enables us to mix our curriculum with real-world knowledge to better prepare our youth."

The NCTAMS LANT program is staffed by nearly 60 volunteer mentors and guest speakers, and services more than 60 youth, 9-12 years of age. Shaw believes the program's success lies in changing the children's attitudes and building their confidence.

"The best reward is the positive feedback we receive annually from parents about their children's participation in DEFY," said Shaw.

The NCTAMS LANT DEFY program also won the Fulcrum Shield award in 2007 for having the best outreach program among military-affiliated youth programs in the nation.



(Left) Sharon Shaw encourages one of the DEFY program's youth in the sit-up competition. (Official U.S. Navy Photo)

CTR2 Reuben Cuenca, NIOC Whidbey Island, briefs VADM Bernard McCullough, commander, U.S. Fleet Cyber Command/U.S. 10th Fleet; on operational procedures during Range Week exercise. (Photo by LCDR James Brokaw)

NIOC Whidbey Island Helps Electronic Attack Aircrews Sharpen Range Skills

By CTR1(SW/AW) Bonnie McCammon, NOIC Whidbey Island

The flights performed by Naval Air Station (NAS) Whidbey Island Electronic Attack aircrews to maintain readiness and flight hours are considered part of a routine cycle in the deployment process. But for Electronic Attack Squadrons (VAQ) 131, 138 and 141, recent flights taking place here were anything but ordinary – they were participating in a ground-breaking exercise called Range Week.

Range Week is the brainchild of Navy Information Operations Command (NIOC) Whidbey Island Commanding Officer, CDR Joseph Pugh, developed to provide Expeditionary VAQ squadrons the opportunity to engage in a series of scenarios imitating the real-world operations that crews can expect to encounter when deployed.

"Range Week offers squadrons the opportunity to sharpen the fine edge of execution before they find themselves in harm's way," Pugh said. "It's something we used to do sparingly with one squadron at a time -- maybe one or two squadrons a year. Now it's a competitive event with multiple squadrons we hope to do at least semi-annually."

The exercise is a unique opportunity for crews to practice 'buttonology' – getting hands-on time with their gear – and engage targets while receiving real-time feedback from NIOC Whidbey Island support personnel. It also encourages friendly competition between the squadrons to see who can complete the assigned objectives most effectively and efficiently.

Squadrons are graded in three areas: pre-mission actions, actual sorties and post-mission actions. Pre-mission actions include aspects of the Concept of Operations (CONOPS), Intelligence preparation and the techniques involved in accomplishing the two. Sorties involved actual flying and execution of Electronic Attack procedures on Communications Electronic Attack gear. Finally, post-mission actions included compilation of after-action reports, lessons learned and associated procedures.

Flights took place over the Vantage Range in Yakima, WA, with NIOC Whidbey Island Fleet Operations personnel coordinating individual events between Yakima and Whidbey Island. Grading was facilitated through a joint effort between NIOC and the Electronic Attack Weapons School. In the end, the Yellow Jackets of VAQ-138 posted the highest marks and was declared the winner.

"This event could not have happened without the full support and buy-in from [Commander Electronic Attack Wing Pacific] CAPT Shay and the squadron skippers," said Pugh.

Commander U.S. Fleet Cyber Command/U.S. 10th Fleet, VADM Bernard McCullough was on hand to witness the inaugural events at the control station in Yakima.

"It was very exciting to have the admiral here, taking interest in this evolution," Yakima team lead, CTR1 Stephen Noreika remarked. "It really underscores the importance of what we're doing out here."

NIOC Misawa Sailors Host Sports Day for Akebono Orphanage Children

Story & Photo by CTI1 Jennifer Johnston

The Sailors of NIOC Misawa have had a long-term relationship with the children of the Akebono orphanage. This year, that relationship was strengthened with a fundraising event and a sports day for next year's graduates.

CTR1 Anthony Melfi headed up the summer fundraising event with the First "Pudding Run" in June. Sailors "sponsored" their favorite runners, and with each donation, the distance they had to run and the amount of pudding they had to eat increased. By the end of the fundraising, all the runners had reached the maximum of six miles and 64 ounces of pudding.

In July, NIOC Misawa hosted a sports day at the Edgren High School Track for the children. LS2 Renee Solis spearheaded that event, organizing a day full of fun. Events included foot races, an egg toss, a tug-of-war, and the favorite, an arm wrestling competition with CTR2 Henry Rogers.

Rogers said, "If the kids had half the fun that I did, I know that they had a great time." An American style barbeque was also prepared to the delight of the Japanese visitors and Sailors alike.

At the end of the day, both the students and the NIOC Misawa Sailors were talking about events planned for the fall and winter.

The day was a great success overall and the children went home happy and tuckered out. The children expressed their excitement in the upcoming events that the Sailors have scheduled for Halloween and Christmas.

Sailors and students line up for an Egg in the Spoon race.

CNO Visits NIOC Texas

By LTJG Peter Crimmins, NIOC Texas Public Affairs

Navy Information Operations Command (NIOC) Texas was recently visited by Chief of Naval Operations (CNO) ADM Gary Roughead. The more than 500 officers and Sailors of NIOC Texas were honored to give the CNO a glimpse into day to day operations at the command.

The mission of NIOC Texas is to support cryptologic and information operations at Texas Cryptologic Center (TCC) in San Antonio as well as providing cryptologic support to deployed Navy tactical assets.

Official U.S. Navy Photo

The visit started off with a coin presentation by the CNO to five Sailors for outstanding performance. CTT1 Paul Wilson and CTN1 Marcella Rax were recognized for spearheading NIOC Texas' Navy-Marine Corps Relief Society effort that raised more than $14,000 towards the $15,000 Greater San Antonio goal. CTR1 Jose Fuentes and CTR2 Lorenzo Phelps received coins for volunteering more than 100 hours to train nine Sailors during the recent reorganization of the Fleet Information Operations Center (FIOC), as well as providing critical indication and warnings to 17 combatants.

Next on the tour agenda was a visit to the TCC Operations Watch Floor, where Roughead witnessed Sailors integrating with their sister services to conduct joint cryptological operations. CTTC John Schoonover and CTI2 Sari Cordova each explained to the CNO how the Navy contributes to the War on Drugs.

The latest reorganization of TCCs joint operations has allowed for greater integration between the services, each bringing a specialty to the fight.

The tour then focused on the evolution of the Navy's involvement in Information Dominance and the rapid growth of cyber. Roughead made it clear that the Navy must be flexible in training new Sailors who are entering the Navy with varying cyber backgrounds.

He also emphasized that the Navy needs ensure that the right people with the right skill sets are placed in the right billets. Roughead said that as the economy begins to recover, the Navy will face the challenge of retaining Sailors with cyber expertise, as the private sector is able to offer attractive jobs and salaries.

TCC site commander, Air Force Col. Hendrickson, thanked Roughead for sending outstanding Sailors to support the command's mission. The CNO thanked Hendrickson in turn for taking care of his Sailors.

As he completed his tour, Roughead thanked CAPT Gregory J. Haws, NIOC Texas' commanding officer, for the outstanding job the command was doing in counter-narcotic operations, as well as pushing the Navy to continue to lead the way in cyber.

NIOC Maryland Sailors Participate in Orioles' "Salute to the Military"

From NIOC Maryland Public Affairs

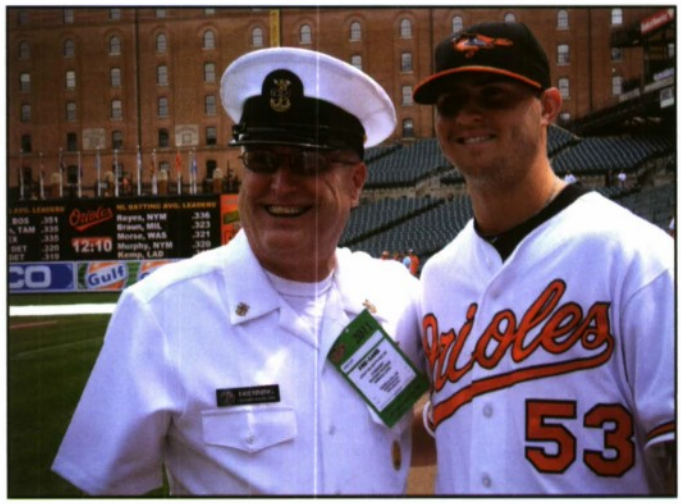
Official U.S. Navy Photos

Navy Information Operations Command (NIOC) Maryland Sailors were guests of the Baltimore Orioles, Aug. 14, as the team celebrated a "Salute to the Military."

Thirty-four of the command's Sailors, guests of the team and pitcher Zach Britton, enjoyed the game from a suite overlooking left field.

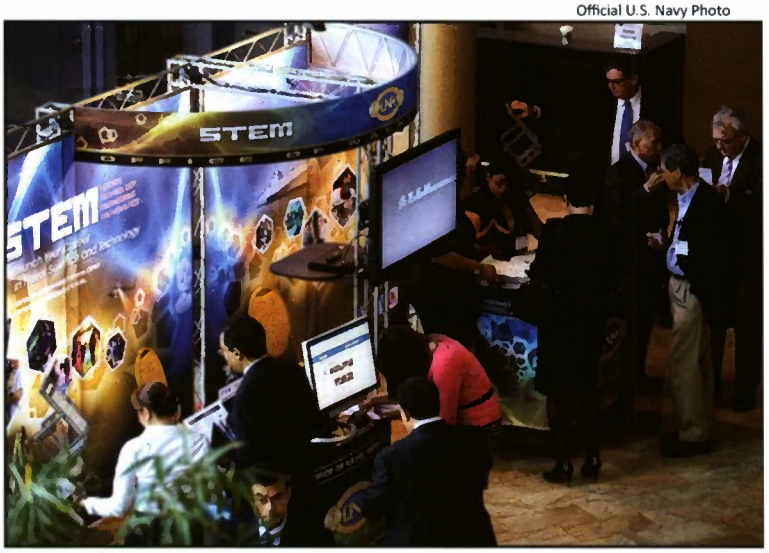
Each Sailor was provided with a pre-game on field pass to meet with the players and coaches from both teams.

NIOC Maryland's color guard paraded the colors and its command choir sang the National Anthem during pre-game festivities. Four members of the Command Choir sang *God Bless America* from atop the Oriole's dugout during the 7th inning stretch. At the same time NIOC Sailors were shown on the park's Jumbotron, displaying a giant American Flag from their suite.



Office of Naval Research Celebrates 65 Years of Pioneering Science & Technology

Official U.S. Navy Photo



From ONR Public Affairs

ARLINGTON, VA -- Unveiling a design for an expansive timeline mural that will showcase the command's history of Science and Technology (S&T) milestones, the Office of Naval Research (ONR) celebrated its 65th anniversary Aug. 1 with a ceremony at its headquarters.

"In the span of a lifetime, technologies from ONR and the Naval Research Lab (NRL) have helped the U.S. Navy and Marine Corps become the pre-eminent maritime and expeditionary force in the world," said Chief of Naval Research, RADM Nevin P. Carr, Jr., who heads ONR. "A great responsibility comes with this legacy to carry on the tradition of innovative, ground-breaking work that will ensure our Sailors and Marines maintain a technological advantage."

NRL Director of Research Dr. John Montgomery underscored ONR's historic impact during a keynote speech to past chiefs of naval research, leaders from partner S&T organizations and members of the naval workforce.

"The products of ONR and NRL have changed the world profoundly and are deeply imbedded in myriad aspects of our everyday life - both military and civilian," Montgomery said. "Yet, as I look to the evolution of scientific and technical endeavors worldwide, I expect our innovations to be invaluable to the nation in the uncertain future we face."

At the urging of American inventor and scientist Thomas Edison, ONR was established in 1923 as NRL. Now ONR's corporate lab, NRL has a history of pioneering work, which includes the first U.S. surveillance satellite, synthetic lubricants for modern gas turbine engines, and the Global Positioning System, or GPS, which revolutionized the science of navigation.

President Harry S. Truman launched ONR on Aug. 1, 1946 with the mission of "planning, fostering, and encouraging scientific research in recognition of its paramount importance as related to the maintenance of future naval power and the preservation of national security."

Today, the command manages the S&T portfolio for the Department of the Navy and provides technical advice to the Secretary of the Navy and Chief of Naval Operations. It executes its mission by funding, through grants and contracts, engineers, physicists, mathematicians, oceanographers, meteorologists and scientists who perform basic research, technology development and advanced demonstrations.

Validating its investments in science and technology, more than 50 researchers have won Nobel prizes for their ONR-funded work.

In the 1940s and 50s, ONR-sponsored researchers developed the first molecular beam machine, currently used by doctors in precision surgeries and procedures, laid the foundation for the Navy's deep-sea submergence program with the record-setting 35,800-foot deep-sea dive of the research vessel Trieste, and engineered microwave amplification by stimulated emission of radiation, or maser, the precursor to the laser.

With the arrival of the 1960s, the naval S&T provider built upon its investment in undersea exploration by funding SEALAB I, II and III, creating experimental habitats to prove humans could exist underwater for extended periods of time.

In 1985, ONR's sonar technology was used to detect the Titanic's wreckage at a depth of nearly 12,500 feet in the Atlantic Ocean, ushering in the age of remotely and robotic underwater vehicles.

Beyond oceanographic exploration, ONR is also focused on meeting emerging challenges. It is investing in Science, Technology, Engineering and Mathematics (STEM) education for future naval innovators, pursuing life-saving medical advances, and researching revolutionary weapons that promise to transform how naval forces fight future battles.

Chief of Naval Operations ADM Gary Roughead believes the Navy and Marine Corps will always look to ONR to deliver "the next big thing" in naval technology.

"Since 1946, the Office of Naval Research and the wider science and engineering community have contributed mightily to our efforts to build the future fleet by providing the technological advantage our Navy needs," Roughead said at a recent conference sponsored by ONR. "And those contributions are rather exceptional today."

About the Office of Naval Research

The Department of the Navy's Office of Naval Research (ONR) provides the science and technology necessary to maintain the Navy and Marine Corps' technological advantage. Through its affiliates, ONR is a leader in science and technology with engagement in 50 states, 70 countries, 1,035 institutions of higher learning and 914 industry partners. ONR employs approximately 1,400 uniformed, civilian and contract people, with additional employees at the Naval Research Lab in Washington, DC.

Naval War College Faculty Member Appointed to 2011-2012 Class of White House Fellows

By CDR Carla McCarthy, Naval War College Public Affairs

NEWPORT, RI -- An information warfare officer, who recently served as a military professor at the U.S. Naval War College (NWC), was one of four service members announced as a 2011-2012 White House Fellow, Sept. 7.

Navy LCDR Theodore Johnson, from Raleigh, NC, departed from NWC in August, where he was a faculty member for NWC's Assist and Assess Team (AAT), teaching and training numbered fleet staffs in Information Operations and Cyberspace Operations for their role in joint operations.

"It is a tremendous honor to have been selected for this prestigious fellowship," said Johnson. "My Fellows classmates are such remarkable people that it really cements in my mind the unique opportunity that this particular fellowship presents."

Johnson is one of 15 Fellows to join the 47th class to serve in the nation's most prestigious program for leadership and public service. They represent a diverse cross-section of professions, including government, business, medicine, education, and the military.

"When I received the call from the Director notifying me that I'd been selected for this year's class, I can't begin describe to you how elated I was," said Johnson. "Knowing that the hard work and introspection paid off is a reward all its own, but there was also an element of pensive reflection."

Every year as many as 1,000 candidates apply for the fellowship. Selection is highly competitive and based on a record of professional achievement, evidence of leadership potential, and a proven commitment to public service.

"While the selection meant that I'd achieved my goal, it also meant that the Commission entrusted me and my classmates with carrying on the program's legacy and being a representative of the President," said Johnson. "Whereas the application process is about showcasing your best, being a Fellow itself is much bigger than that. Our class is committed to living up to this responsibility."

Johnson was placed with the Energy Department, where he will gain an unparalleled experience working with senior administration officials on ever-changing issues and challenges.

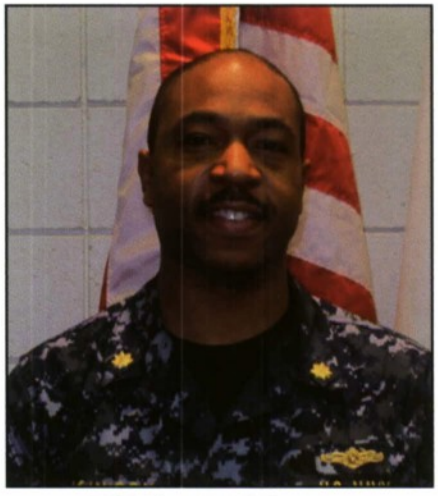
"Because the long process of becoming a fellow, from application to regional interviews to selection weekend, is so intense and comprehensive, my first day being a Fellow was surreal," said Johnson. "But it was much like the feeling experienced at certain points in a naval career: the day you're commissioned, the day you complete your first deployment, or even the first day you get to wear your uniform with your warfare device or newest personal award medal. Just as in the Navy, we enjoy the moment, we but don't dwell on it, because there is more to be done."

Johnson's thirteen years of commissioned service include numerous afloat deployments throughout Asia and the Middle East, cyberspace operations supporting major combat operations, and as aide-de-camp to the Director of the National Security Agency. In 2007, Johnson deployed with Expeditionary Strike Group SEVEN in support of Operation Sea Angel II, the disaster relief response to Cyclone Sidr in Bangladesh, and in 2009, he conducted research in Africa, Asia, and South America that led to official U.S. Navy publications on theater security cooperation.

"Though the mission is fairly new to me, the technical and leadership experience the Navy has afforded more than prepares me for the tasks ahead," said Johnson.

Education and community service are also key components of the White House Fellows program.

"In addition to this placement (with the Energy Department), the Fellowship program has a series of seminars with Cabinet officials, public and private sector senior leaders, and many others that provide a unique insight into the workings of our government and our country," explained Johnson, who holds a Bachelor of Science from Hampton University and a Master of Liberal Arts with an International Relations concentration from Harvard University.



LCDR Theodore Johnson

Created in 1964 by President Lyndon B. Johnson, the White House Fellows Program is designed to give promising American leaders "first-hand, high-level experience with the workings of the federal government, and to increase their sense of participation in national affairs," according to a White House statement.

The program is intended to encourage active citizenship and a lifelong commitment to service. Johnson joins an accomplished group of over 600 White House Fellows alumni, including former Labor Secretary Elaine Chao, former Secretary of State Gen. Colin Powell, U.S. Sen. Samuel Brownback, U.S. Rep. Joe Barton, retired U.S. Army Gen. Wesley Clark, retired ADM Dennis Blair, ADM Patrick Walsh and VADM Ann Rondeau.

"Though it's my name on the Fellowship website, this accomplishment belongs to so many people," said Johnson. "My family and friends have been an immeasurable source of support and encouragement, but it also belongs to my shipmates who I've served with, who gave me confidence, who prepared me for interviews, and who were just as committed to my selection as if it were them."

"I will miss the camaraderie of the wardroom and shipmates during this Fellowship year, but I intend to make the most of it, make them proud, and return to the Fleet a better naval officer as a return on their, and the nation's, investment."

Special Recognition

LEGION OF MERIT

CAPT William Chase, NCTS Guam
CAPT Katherine Donovan, CYBERFOR VA Beach
CAPT Stephen Frick, NASA JCS
CAPT Diane Gronewold, NIOC Suitland
CAPT Daryl Hancock, COMTENTHFLT Ft Meade
CAPT Paul Jaeger, COMTENTHFLT Ft Meade
CAPT Gregory James, NIOC Texas
RADM Thomas Meek, CYBERFOR VA Beach

DEFENSE MERITORIOUS SERVICE MEDAL

CTRC Tracey Irvin, CSG, US Forces Korea
CWO3 Christopher Williams, NIOC Maryland

MERITORIOUS SERVICE MEDAL

CAPT Angela Albergottie, NETWARCOM VA Beach
CAPT John Archer, NR NIOC Georgia
CDR William Baas, NR NIOC GA Detroit
CTRCS Robert Boyd, NIOD Digby
CDR Michael Dewalt, CYBERFOR VA Beach
CMDCM Jacqueline Dirosa, CYBERWARDEVGRU
CDR Michael Farren, NIOC Hawaii
CDR Vanessa Hamm, COMUSTENTHFLT Ft Meade
CDR Nicholas Homan, NIOC Colorado
LCDR Laura Jefferies, NIOC Suitland
CMDCM William Keith, NIOC Colorado
LCDR Lemuel Lawrence, COMTENTHFLT Ft Meade
CDR Bryan Lopez, NIOC San Diego
CMDCM James Mathews, NCTAMS PAC Wahiawa
CDR Timothy May, NIOC Menwith Hill
CAPT Kenneth McKown, NIOC Norfolk
CWO5 James Morris, Jr., NIOC Hawaii
CDR John Myers, NIOC Maryland
CAPT Robert Rivera, NR NNWC VA Beach
CAPT Steven Simon, NCMS Washington, DC
CDR Christopher Taylor, NIOC Norfolk
NCCM Gary Taylor, NIOC Georgia
LCDR Paul Wilkes, NIOC Norfolk

AIR MEDAL

CTI2 Heather Burns, NIOC Bahrain
CTI2 Johnathan Debord, NIOC Bahrain
CTI2 Benjamin Fewkes, NIOC Bahrain
CTI1 Anwar Goins, NIOC Bahrain
CTI1 Aaron Penk, NIOC Bahrain
CTR1 Joshua Robishaw, NIOC Bahrain
CTI1 Jason Sikora, NIOC Bahrain
CTR1 Matthew Strauss, NIOC Bahrain
CTI1 Anthony Walter, NIOC Bahrain
CTI1 Christian Wertman, NIOC Bahrain

JOINT SERVICE COMMENDATION MEDAL

CTR2 Ernie Arciga, NIOC Hawaii
CTTC Erik Barrera, NIOC Colorado
CTI1 Matthew Blaszczyk, NIOC Maryland
IT1 Melissa Caban, NIOC Hawaii
CTI2 Brian Chalfant, NIOC Hawaii
CTI1 Derek Dalton, NIOC Maryland
IT1 Dean Gerali, NIOC Sugar Grove
LT Stephen Gray, NATO Training Mission Afghanistan
CTTC Andrew Hodyl, NIOC Colorado
IT3 Adam Kissinger, SUSLA Korea
LCDR Sven Krauss, NIOC Maryland
CTRC Victor Parrish, NIOC Sugar Grove
CTR1 Laurel Schwindenhammer, NIOC Sugar Grove
CTI1 Don Tillman, NIOC Sugar Grove
CTR1 Terry Wells, NIOC Sugar Grove

NAVY AND MARINE CORPS COMMENDATION MEDAL

LCDR Frederick Alegre, NR NIOC Norfolk
QMCS Christopher Allor, NETWARCOM VA Beach
LTJG Lance Alt, NIOC Texas
YNCS Donella Anderson, NIOC Hawaii
CTN1 Bernard Armer, NIOC Norfolk
CWO3 Richard Aubin, NIOC Georgia
LT Peter Avitto, CYBERFOR VA Beach
CTTC Michael Baauw, NR NIOC Detroit
ITCM Patricia Barlow, NCTAMS LANT
CTR1 Kimberly Barth, NIOC Whidbey Island
CTT1 Kenneth Batten, NAVNETCENWARGRU Pensacola
CTT1 Charles Biles, NIOC Misawa
ITCS Arron Boone, CMS TEAM Yokosuka Japan
CTR1 Scott Bossard, NIOC Texas
NCC Antonio Botello, NIOC Texas
LCDR Greg Braaten, COMTENTHFLT Ft Meade
LTJG William Brinkmeyer, NIOC Hawaii
CWO4 Peter Brklycica, NIOC San Diego
LT Kenneth Brooks, CYBERFOR VA Beach
LCDR Ian Brown, NCDOC VA Beach
CTR1 James Brown, NIOC Suitland
CTNCS Joel Brown, COMTENTHFLT Ft Meade
ITCS Davy Burleson, NCTAMS PAC
MM1 Joaquin Cadena III, NIOC Maryland
CTIC Shavonne Castro, NIOC Texas
ITC Sharon Clark, GNOC Det Norfolk
CTNC Tamika Cobb, NIOC Norfolk
LCDR Derek Cole, NIOC Misawa
CTI1 Jasen Cooper, NIOC Maryland
ITC Randall Crabtree, GNOC Det Norfolk
CTRCS Craig Cross, NIOC Texas
LCDR Jose Cruz, Jr., NCTS Jacksonville
CTI1 Jon Cryor, NIOC Maryland
YN1 Donald Dattalo, Jr., CYBERFOR VA Beach
CTIC Pamela De Voto, NIOC Bahrain
ETC Timothy Dooley, CYBERFOR VA Beach
ITC David Dufour, CMS TEAM Camp Lejeune
CTIC Shenequa Dunn, NIOC Hawaii
CWO3 Timothy Echeverio, NIOC Whidbey Island
CTI1 Karen Eggers, NIOC Maryland
CTR1 Silvano Elizondo, NIOC Texas
LT Anthony Ellis, NCTS Naples
LT Paul Felsing, II, NIOC Georgia
LCDR David Filanowicz, NCDOC VA Beach
LCDR David Fletcher, NIOC Georgia
CDR Claudi Flores, CYBERFOR VA Beach
YN1 Steven Foran, NIOC Texas
CTT1 Fredrick Foutz, NIOC Texas
CTR1 Andrew Frazure, NIOC Texas
LN1 Misty Galentine, NIOC Hawaii
CTIC Kasey Gallardo, NIOC Texas
CTNC David Garcia, NIOC Suitland
LT Brian Gardler, NCDOC VA Beach
LCDR James Gartside, NR NIOC Maryland
CTRCS William Gaudreau, NIOC Yokosuka
CTRCS Matthew Genovese, NIOC Hawaii
CWO3 Patrick Gentry, NCTAMS PAC Wahiawa
IT1 Jimmy Gipson, NCTS Far East Det Misawa
LT John Glaze, CYBERFOR VA Beach
CTRC Benjamin Godby, NIOC Bahrain
LSCS Yolanda Gooding, NIOC Norfolk
CTRCS Karl Grubic, NIOC Hawaii
ITC Paul Guidry, NIOC Maryland
CTTC Gregory Harmon, COMTENTHFLT Ft Meade
CTIC Ted Hellene, NIOC Maryland
ETC Corey Henderson, NCTS Bahrain
ET1 Jose Hernandez, NCTAMS PAC Wahiawa
CTICM Brendan Hiers, NIOC Texas
LCDR Paul Hughes, NCTS Bahrain
CTI1 Jeffrey Japinga, NIOC Maryland
CTRCS Peloquin Jonathan, CYBERFOR VA Beach
CWO3 Patrick Jones, NCTS Far East Det Misawa
LT Philip Keith, NCTAMS PAC Wahiawa
CWO3 Albert Keller, NNWG FT Meade
MAC Heather Kilday, NCTAMS PAC Wahiawa
CTRC Michael Kling, Jr., NIOC Hawaii
LT Daniel Krowe, NIOC Maryland
CTRC Julius Lamonica, NIOC Texas
ITC Scott Lauren, NCTAMS LANT Det Rota
ITC Lonnie Lavalais, NCTAMS LANT Norfolk
LTJG Aaron Lawson-Gradle, NIOC Georgia
CTR1 Mathew Leetch, NIOC Bahrain
YN1 Marty Levant, COMNETCENWARGRU Ft Meade
LT Bryan Luallen, NIOC Pensacola
CWO4 Sheldon Malone, CYBERFOR VA Beach
CTT1 Salvador Martinez, NIOC San Diego
LT Jonathan McCarter, NIOC Norfolk
CWO5 Montana McClanahan, GNOC Det Norfolk
CWO4 Laurence McGowan, CYBERFOR VA Beach
LCDR Richard Menard, NCMC Washington, DC
ITCM Sheila Menge, NCTS Bahrain
CTRC Frank Migliaccio, NIOC Suitland
LCDR Kenneth Moates, NIOC Georgia
CTRC Gabriel Moore, NIOC Texas
YN1 Angela Myles, NIOC Texas
CTICS Kelly Parks, NIOD Kaneohe Bay
CTICS Kenneth Paulsen, NIOC Georgia
MCC James Perkins, NETWARCOM VA Beach
CTRCM Edwin Purdy, NIOC Yokosuka
CTI1 Greggory Radach, NIOC Maryland
ITCS David Rebertus, NAVMARSPECCN Bahrain
IT2 Christopher Reed, NCTAMS PAC Wahiawa
ETCS Kenneth Reynolds, NCTS Naples
CTRC Kenneth Richter, NIOC Bahrain
LCDR Jonathan Rinkus, CYBERFOR VA Beach
IT1 Ray Robertson, NCTS Naples
CWO3 Donald Robinson, NIOC Suitland
CTRC Alexander Rojas, NIOC Suitland
CTRC Sibyl Rostchild, NAVNETCENWARGRU Pensacola
LCDR James Rowland III, CYBERWARDEVGRU Ft Meade
YN1 Zakiyyah Saleem, NIOC Georgia
CTI1 Brian Schooley, NIOC Hawaii

ICC Stephen Shallberg, NCTAMS LANT Det Rota
MAC Bruce Simmons, NIOC Norfolk
CTRCM Kyucca-Ali Simpson, NIOC Hawaii
CTIC Amy Smith, NIOC Georgia
CTIC Jonathan Smith, NIOC Maryland
IT1 Susannah Staples, NCTAMS LANT DET Hampton Roads
CTT1 Mark Svatek, NIOC Hawaii
IT1 Kenneth Trosper, NCTAMS LANT Norfolk
LCDR Henry Vegter, Jr., NIOC Pensacola
LCDR Joshua Vergow, COMUSTENTHFLT Ft Meade
ITC William Vue, NCTS FAR EAST DET Misawa
LT Brian Walsh, NIOC Maryland
CWO3 Danny Walton, CYBERFOR VA Beach
CTIC Michael Wang, NIOC Misawa
CTIC Melvin Welker, NIOC Maryland
CTIC Tricia Whitmire, NIOC Misawa
CTICS Vincent Whitmire, NIOC Misawa
CTN1 Kristi Windham, NIOC Suitland
ITC Eric Wishard, CYBERFOR VA Beach
CTRC Patrick Wolfrey, NIOC Maryland
CTI1 Jerome Yoon, NIOC Maryland
ITC Phillip Zarate, NCTAMS PAC Wahiawa

JOINT SERVICE ACHIEVEMENT MEDAL

CTN2 Joseph Arbo, NIOC Maryland
LT Clint Brown, NIOC Hawaii
CTI2 Janelle Chouinard, NIOC Georgia
CTR2 Nicholas Fenz, NIOC Texas
ITSN Markus Galloway, SUSLA Korea
CTI1 Tracie Hoops, SUSLA Korea
IT3 Stephanie Jones, NIOC Hawaii
CTT2 Abel Montemayor, NIOC Texas
CTN2 James Mullen, NIOC Maryland
IT3 Ashley Peterson, NIOC Hawaii
CTR2 Anthony Petrillose, NIOC Texas
CTI2 Bryan Ransom, NIOC Hawaii
IT3 Matthew Robertson, NIOC Hawaii
CTI2 Jacilyn Taggart, NIOC Georgia
YN3 Justin Turner, NIOC Maryland

NAVY AND MARINE CORPS ACHIEVEMENT MEDAL

IT2 Daniel Ailes, NCTS San Diego
IT1 Matthew Alford, NCTSC Oklahoma City
CTI1 Corey Allen, NIOC Bahrain
CTI2 Kelly Allen, NIOC Texas
CTM1 Carlos Alvarez, NIOD Groton
IT2 Vincent Amos, NCTS San Diego
CTI2 Michael Anderson, NIOC Texas
CTR1 Melissa Andrews, NIOC Norfolk
ET1 Clestian Andrieux, Jr., NCTS Det Sicily
CTRC Pleshette Askew, NR NIOC Maryland
CTN2 Sarah Baalbergen, NIOC Georgia
CTR2 Zachary Bailey, NIOC Hawaii
CTM2 Paul Barban, NIOC Maryland
CTI1 Hilda Barfield, NR NIOC Maryland
ET2 Rachel Barman, NCTAMS LANT Norfolk
CTT2 Mark Barrett, NIOC Hawaii
LS2 Joshua Baucom, NIOC Georgia
IT3 Donald Besch, NCTAMS PAC Wahiawa
CTT1 Christopher Binning, NIOC Georgia
CTR1 Joseph Bishop, NIOC Texas
CTI2 Edwin Blanton, NIOC Texas
CTI1 Richard Blatt, NIOD Kaneohe
CTM2 Anthony Blevins, NCTS Guam
LT John Bogdan, III, NIOC Yokosuka
IT3 Sean Bond, NCTS Naples
CTR3 Axton Bonsey, NIOC Georgia
CTR2 Gasper Bontempo, NIOC Maryland
CTI1 Melissa Boots, NIOC Maryland
CTR1 Norma Braden, NIOC Hawaii
CTM2 Phillip Bratton, NIOC Hawaii
IT1 Joshua Brice, NIOC Hawaii
CTN2 Michael Britton, NIOC Norfolk
CTI2 Beau Broussard, NIOC Texas
IT1 Georgia Brown, NCTAMS LANT DET Hampton Roads
CTR1 Vernon Brown, NIOC Texas
IT1 Kent Bryant, NR NIOC HI-Ogden
IT1 Javon Burden, NCTS San Diego
LCDR Joshua Burkholder, NCTS San Diego
CTI2 Heather Burns, NIOC Bahrain
ET1 Christopher Burton, NR SPAWAR 466
IT1 Ronald Butler, NCTSC Det Oklahoma City
IT1 Courtney Cain, NCTS Naples
CTRCS Joseph Cantu, NIOC Maryland
CTR1 Ernest Cardwell, NIOC Texas
CTR2 Molly Carpenter, NIOC San Diego
CTI2 Devin Carroll, NIOC Maryland
IT1 Christopher Castillo, NCTS Guam
IT2 Ashley Castleberry, NIOC Hawaii
CTR2 Irene Cencich, NIOC Misawa
CTI1 Kelly Chambers, NIOC Maryland
CTR2 Christopher Chapa, NIOC Hawaii
IT2 James Choe, NCTS Sicily
CTI1 Nicole Choquette, NIOC Maryland
CTR2 Kenneth Clark, Jr., NIOC Hawaii
LN1 Richard Cocklin, COMFLTCYBERCOM Ft Meade
CTM2 Michael Cohen, NIOC Norfolk
LT Patrick Condren, NIOC Yokosuka
YNSN Christopher Coogan, NIOC Yokosuka
CTI2 Ryanne Cook, NIOC Texas
YN1 Antoine Curry, NCTS Far East Yokosuka
CTRSN Nolan Dabruzzi, NIOC Hawaii
CTI1 Matthew Dasilva, NIOC Hawaii
IT1 Gregory Davis, NCTAMS LANT Det Hampton Roads
CTRC Jason Davis, NIOC Texas
IT1 Holly De Los Santos, NIOC Hawaii
CTI2 Johnathan Debord, NIOC Bahrain
LT Stacey Demick, NCTAMS LANT Norfolk
CTMSN Clint Denton, NIOC Norfolk
IT2 Hilton Deshields, NCTAMS PAC Wahiawa
YNC Jenean Dickens, NCTS San Diego
CTR2 Benjamin Diseroad, NIOC Hawaii
IT1 Julian Dixon, NCTSC Oklahoma City
CTRC Cynthia Dodd, NIOC Yokosuka
LT Joseph Duchesneau, COMTENTHFLT
CTR3 Maxwell Duncan, NIOC Maryland
CTT1 Nicole East, NIOC San Diego
CTM1 Ricardo Espinoza, NIOD Groton
LT Jessica Fahrman, CYBERFOR VA Beach
IT2 Paloma Faircloth, NCTAMS PAC Wahiawa
CTRC Daniel Farnsworth, NIOC Hawaii
CTI2 Kevin Farr, NIOC Texas
ET1 Dustin Farris, NCTS Sicily
CTT1 Joshua Feenstra, NIOC Hawaii
IT1 Mark Ferguson, Jr., GNOC Det Norfolk
CTT2 Brian Finley, NIOC Hawaii
LTJG Scott Finley, NIOC Georgia
CTR2 Derek Folkers, NIOC Suitland
CTT2 Michael Foster, NIOC Hawaii
CTM1 Charles Frederick, NIOC Hawaii
LTJG Corey French, NR NIOC Maryland
CTR2 Justin French, NIOD Chesapeake
CTM1 Wade Friedrich, NIOC Norfolk
IT2 Michael Fry, NCMS Washington DC
CTR1 Jason Fullmer, NIOC Texas
IT2 Ignacio Gachuzo, NCTS Naples
YN2 Roshon Gardner, NIOD Groton
CTI1 Richard Gaston, NIOC Texas
IT1 Tyler Gauthier, NCTS Naples
CTR1 Laura Geigel, NIOC Maryland
IT3 Stephen Gerrald, NIOC Norfolk
CTTC Derrick Gillespie, NIOC Texas
CTR1 Eileen Girardy NIOC Georgia
OS2 Jessica Glumm, NCTAMS PAC Wahiawa
CTI1 Anwar Goins, NIOC Bahrain
IT1 Christopher Gonsalves, NCTAMS LANT Norfolk
CTN1 Anthony Gonzales, NIOC Hawaii
IT2 Emmanuel Gonzalez, NIOC Texas
CTR1 Teresa Gore, NIOC Pensacola
CTI2 Kaleb Goss, NIOC Texas
LT Michael Gossett, NR NIOC Texas, St Louis
EN2 Royce Greenwood, NCTS Sicily
CTR2 Antonio Guidry, NIOC Hawaii
CE3 Dusten Haberle, NCTS Naples
LS2 Afeerah Haimanchandra, NIOC Sugar Grove
CTI1 Beth Hammond, NIOC Maryland
IT1 Rocio Hammond, NCTS Jacksonville
IT1 Jeffery Hansen, NMCI Det Norfolk
IT2 Tranette Harbin, NCTS Sicily
YN2 Soraida Harper, NIOC Georgia
CTI1 William Harris, NIOC Georgia
CTRSN Jordan Hartke, NIOC Hawaii
CTR1 Cory Hays, NIOC Georgia
LTJG Kevin Heatherly, NIOC Georgia
CTI2 Justin Heise, NIOC Misawa
CTR2 Michael Helgerson, NIOC Hawaii
YN2 Omar Henry, NCTS San Diego
ISCS Richard Heppard, SPAWAR
IT2 Sarai Hernandez, NCTS San Diego
LT John Hessey, CYBERFOR VA Beach
CTT2 Phillip Higgins, NIOC Hawaii
CTI1 Alexis Hileman, NIOC Hawaii
YNSN Larrece Hills, NCTS Naples
CTT1 Darrell Hitchcock, NIOC Norfolk
BU1 Jason Hoak, NIOC Hawaii
CTR2 Dustin Hoesly, NIOC Hawaii
CTR1 Andrew Hoffman, NIOC San Diego
LS2 Crystal Holbrook, NCTAMS PAC Det Puget Sound
CTT1 Luis Holguin, NIOC Hawaii
CTI1 Margery Holston, NIOC Bahrain
LTJG Jason Hooper, NIOC Texas
CTI2 Camera Howard, NIOC Texas
IT1 Sanford Howell, NCMS Det San Antonio
CTTC William Howeth, NIOC San Diego
CTI1 Lindsay Hoying, NIOC Bahrain
LT Adam Humphrey, NIOC San Diego
CTI2 Geoffrey Hutchinson, NIOC Maryland
IT2 Sasha Hutchinson, NCTAMS PAC Wahiawa
ET2 Luis Ibanez, NRTF NISCEMI Sicily
CTI1 Roberto Ibarra, NIOC Texas
IT1 Renee Ingram, NCTS San Diego
ET2 Damien Jackson, NIOC San Diego
CTR2 Jermaine Jackson, NIOC Hawaii
CTR2 Ryan Jackson, NIOC Texas
CTM1 Shannon Jackson, NIOC Bahrain
CTR3 Travis James, NIOC Texas

CTI1 Nathaniel Jarred, NIOC Maryland
CTR3 Michael Jones, NIOC Suitland
CTTC Leon Jordan, Jr., NIOC Yokosuka
CTNCS Anthony Joyce, NIOC Maryland
LS1 Thomas Joyce, NCTAMS PAC Wahiawa
CTN1 Ronald Judy, NCDOC VA Beach
CTR1 Rosie Kasem, NIOC Hawaii
CSC George Keene, NIOC Maryland
CTNC Jeffrey Kelley, NIOC Texas
CTI2 Collen Kelton, NIOC Misawa
CTR2 Andry Kenith, NIOC Misawa
CTR2 Wesley Kennedy, NIOC Bahrain
IT2 David King, NMCI Det San Diego
CTM1 Dirby Knopik, NIOD Groton
CTT2 Sean Kontogianis, NIOC Hawaii
CTR2 Justin Kudlacik, NIOC Hawaii
NC1 Shannun Lamorte, NIOC Norfolk
CTI2 Timothy Landrum, NIOC Georgia
LS1 David Leflet, NIOC Hawaii
CTT1 Frakelia Leonard, NIOC Georgia
CTI1 Qing Liang, NIOC Hawaii
LTJG Jeremy Linton, NIOC Texas
CTI1 Jason Loftin, NIOC Maryland
IT1 Lovmika Long, NMCI DET San Diego
IT3 Trea Long, NCTS Sicily
LT Juan Luna, NCTS San Diego
CTR1 Alexis Lund, NIOD Kaneohe Bay
CTT1 Richard Lupson, NIOC Hawaii
CTI1 Michelle Lynch, NIOC Georgia
CTR2 Brett Macklin, NIOC Hawaii
CTR3 Warren Maddox, NIOD Chesapeake
IT2 Frank Madu, NCTSC Det Fairfield
CTR1 Jarrod Malkin, NIOC Bahrain
CTNC Allyn Malventano, NCDOC VA Beach
CTI1 Byron Markley, NIOC Bahrain
IT3 Randi Martin, NIOC Maryland
CTT1 Salvador Martinez, NIOC San Diego
CTT1 Joshua Mathison, NIOC San Diego
CTM1 Brent McMillen, NIOD Groton
ENS Erin McNamara, NIOC Maryland
CTR2 Courtney Meisenheimer, NIOC Georgia
LS2 Derek Meyers, NCTAMS PAC Wahiawa
CTR1 David Miller, NIOC Texas
CTR2 Kelsey Moretti, NIOC Norfolk
CTT1 Jed Morris, NIOC Yokosuka
CTI1 Diana Morrison, NIOC Texas
ET3 Daniel Moseley, NCTAMS LANT DET Rota
CTI1 April Mulé, NIOC Misawa
YNSN Quinton Nabors, NIOC Sugar Grove
CTI1 Michael Neal, NIOC Texas
CTT2 Zachary Nelson, NIOC Hawaii
IT2 Todd Newell, CYBERFOR VA Beach
Cpl Brian Nine, USMC, NIOC Hawaii
IT3 John Nugent, NCMS Washington DC
LT Ryan O'Connell, COMTENTHFLT Ft Meade
LT Nicholas O'Conner, NIOC Georgia
ETC Mark O'Dell, NCTSC Oklahoma City
CTI1 Erin Olson, NIOC Menwith Hill
CTN2 Greggory Park II, NIOC Maryland
CTI2 Shasta Parker, NIOC Georgia
LTJG William Parker, NIOC Hawaii
CTR1 Jarred Parrott, NIOD Digby
CTR2 Bryan Parsons, NIOC Hawaii
CTI2 James Payne, NIOC Texas
MM2 Ronald Pecoraro, NIOC Maryland
ITC Richard Perkins, NCTS Jacksonville
LTJG Brian Peterson, NIOC Hawaii
LCDR John Phillips, NETWARCOM VA Beach
IT2 Cole Picard, NCTAMS LANT Norfolk
CTI1 Kristin Pierce, NR NIOC Camp Parks
CTM2 Craig Pitcher, NIOC Norfolk
CTN1 Garth Plouzek, NIOC Pensacola
ET2 David Porter, NCTS Jacksonville
CTN2 Gregory Price, NIOC Hawaii
CTR2 Daniel Pries, NIOC Hawaii
CTR2 James Pufahl, NIOC Hawaii
CTR1 Joshua Pugh, NIOC Hawaii
CTR2 Tia Queen, NIOC Suitland
LTJG Sarah Quemada, NIOC Texas
CTI2 Sarah Ramage, NIOC Texas
CTR1 Al Ramon, NIOC Texas
ET2 Stephan Raymond, Jr., NCTAMS PAC Wahiawa
CTR3 Brandon Rea, NIOC Georgia
CTM1 Rashaad Reid, NIOC Norfolk
IT3 Aaron Richards, NCTS Naples
CTR1 Damien Richardson, NIOC Hawaii
IT1 Edward Richman, NCTS Jacksonville Det Key West
CTM1 Jerrod Rickard, NIOC Yokosuka
CTI3 Dani Ridgway, NIOC Texas
IT1 Joshua Rinaldi, NMCSO Europe Naples
LTJG Alexander Rios, NIOC Hawaii
LTJG Ian Roberts, NR NIOC HI Tacoma
IT1 Theresa Robles, NCTS Sicily
LS2 Marcela Rodriguez, NIOC Maryland
ET1 Samuel Rodriguez, NCTS Jacksonville
CTIC Catherine Ronco, NIOC Hawaii
YN1 Lakesha Rose, NCTS Sicily
CTR2 Fidencio Rubalcava, Jr., NIOC Misawa
CTR2 Nathan Rumph, NIOC Hawaii
CTI2 Amanda Ruthven, NIOC Maryland
LS1 Pierre Saint-Pierre, NETWARCOM VA Beach
CTT1 Adam Salsbury, NIOC Hawaii
Maj Thomas Sammel, USMC, NIOC Hawaii
LT Carrie Sanders, NIOC Hawaii
CTR2 Trevor Sanders, NIOC Hawaii
ET1 Anthony Schmakel, NCTAMS PAC Det Puget Sound
LTJG Michael Schmidt, NIOC Maryland
IT2 Bryan Schmitt, NCDOC VA Beach
ET2 Frank Schuh, NCTS Far East
IT2 Chelsey Schumaker, NCTS Naples
IT2 Aimee Scott, NIOC Yokosuka
YN1 John Sears, Jr., COMTENTHFLT Ft Meade
ISC Brian Shields, CYBERFOR VA Beach
CTR1 Kendell Shinmori, NIOC Suitland
LT Jonathan Sholtis, NIOC Maryland
CTR1 Amanda Silvestro, NIOC Menwith Hill
CTR2 Kezia Simmons, NIOC Hawaii
CTN1 Seth Simmons, NCDOC VA Beach
IT3 Kurtis Slaugenhaupt, NCTS San Diego
Maj Michael Slawski, USMC, NIOC Hawaii
IT1 Aquarius Smith, NIOC Norfolk
CTR1 Arion Smith, NIOC Misawa
ET2 Christopher Smith, NCTAMS PAC Wahiawa
CTR1 James Smith, NIOC Suitland
CTR2 Kimberly Smith, NIOC Hawaii
LT Richard Smith, NR NIOC Washington
IT1 Toby Smith, NMCI Det San Diego
CTR1 Mark Snoddy, NIOC Bahrain
CTI1 Steven Sorkin, NIOC Georgia
CTN1 Roderick Sparks, NIOC Norfolk
ET1 Chadwick Spradling, NCTSC Det Patuxent River
IT3 Codi Starks, NCMS Washington DC
CTN1 Daniel Steiner, NETWARCOM VA Beach
CTNC Tammy Sternberg, NCDOC VA Beach
EO1 Donald Stone, NIOC Sugar Grove
LCDR Luciana Sung, COMTENTHFLT Ft Meade
LTJG Jason Tews, NIOC Hawaii
CTR1 James Thieman, NIOC Maryland
CTM2 John Thompson, NIOC Hawaii
CTN1 John Thompson, NIOC Suitland
LT Eamonn Tigani, NIOC Yokosuka
CTI1 Justin Tockey, NIOC Hawaii
IT3 Rogelio Torres, NCTAMS PAC Wahiawa
CTT1 Lucia Treto, NIOC Hawaii
CTN2 John Trevino, Jr., NIOC Pensacola
CTR2 Nelissa-Joy Trinh, NIOC Suitland
CTT1 Justin Tropp, NIOC Hawaii
CTI1 Susan Truong, NIOC Hawaii
CTI2 Ashley Turjanica, NIOC Georgia
LS2 Teslin Turley, NCTAMS PAC Wahiawa
Capt Steve Urrea, USMC, NIOC Hawaii
YN2 Jason Ussia, NIOC Bahrain
IT2 Gary Vallejo, NIOC Georgia
CTT2 Charlene Vasquez, NIOC Hawaii
CT2 Tiffany Vimpany, NIOC Hawaii
IT2 Brian Virgili, NCDOC VA Beach
CTI2 Josylin Waggener, NIOC Texas
BM1 Mark Wallace, NIOC Norfolk
CTT2 Roy Welch, Jr., NETWARCOM VA Beach
CTR1 William Whaley, NIOD Digby
CTI1 Bailey White, NIOC Misawa
CTR2 Ryan White, NIOC Hawaii
CTR3 Jeffrey Whitney, NIOC Maryland
Maj Brian Wilcox, USMC, NIOC Hawaii
IS3 Mary Williams, NIOC Norfolk
CTI1 Robert Williams, NIOD Seoul
IT3 Stephen Williams, NCTS Williams
CTT2 Thomas Willingham, NIOC Georgia
CTR2 James Willis, NIOC Hawaii
CTR1 Jon Wilson, NIOC Hawaii
CTT2 Pearce Wilson, NIOC Yokosuka
IT3 Jacob Wright, NCMS Washington DC
IT1 Twila Wright, NCTAMS LANT Det Hampton Roads
IT1 Patrisha Wyatt, NCTAMS LANT Det Hampton Roads
YNSN Michael Yates, NIOC Georgia

MILITARY OUTSTANDING VOLUNTEER SERVICE MEDAL

CTT1 Clayton Braswell, NIOC Georgia
IT1 Dean Gerali, NIOC Sugar Grove
CTN1 Randall Lazarus, NIOC Pensacola
AT1 Joseph Nevis, NR SPAWAR
YN1 Zakiyyah Saleem, NIOC Georgia
CTRC Merrill Tilley, NIOC Misawa
CTR1 Shamika Wheaton, NIOD Yakima

CIVILIAN LENGTH OF SERVICE AWARDS

Bradley McNamar, CYBERFOR VA Beach - 20 Years
Sandra Bickham, CYBERFOR VA Beach - 25 Years
Sharon Shaw, CYBERFOR VA Beach - 30 Years

Intelligence Director Recognizes USCYBERCOM Junior Sailor of the Year

(Right to left) Director of Intelligence (J2), U.S. Cyber Command, RADM Samuel J. Cox, presents the CYBERFOR 2010 Junior Sailor of the Year award to IS3 Joseph Biondo at quarters in July. Biondo is an imagery analyst assigned to CYBERFOR Fleet Intelligence Detachment, Washington, DC, Office of Naval Intelligence. The presentation took place upon Biondo's return from his USS Carl Vinson (CVN 70) deployment. Biondo also received a Letter of Commendation from the Carl Vinson. (Photo by Alex M. Cavazos)

Hope Award Winner Announced

From Chief of Naval Personnel Public Affairs

WASHINGTON, DC -- The Navy recently announced that CTR1 (IDW/SG/SW/AW) Jamar J. Salters, of Navy Information Operations Command (NIOC), Hawaii, is the 2010 Spirit of Hope Award winner.

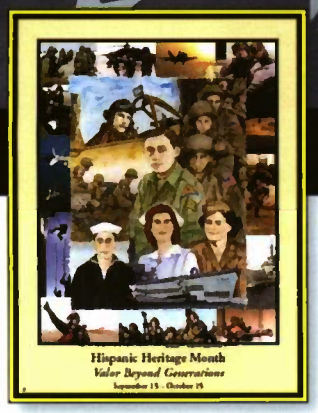
The award will be presented to Salters at a Pentagon ceremony honoring awardees of all five military services Nov. 15.

Established in 1997, the Spirit of Hope Award is presented by the Wiegand Foundation in honor of the famed entertainer and supporter of military personnel, Bob Hope. The award is presented to individuals or organizations that embody Hope's commitment and service to the men and women of the military. A Navy Sailor or civilian has been honored with this award every year since 2005.

Salters was nominated by the commanding officer of NIOC Hawaii for his "selfless devotion, dedication, and commitment to helping more than 3,300 Sailors reach their educational and professional goals."

The award citation also notes that Salters motivated fellow Sailors to get involved in community service. His involvement in nine volunteer fundraising, educational and community projects demonstrates his support to the community.

Official U.S. Navy Photo



Hispanic Commmunity Enriches Our Country Beyond Measure

From Armed Forces Press Service

National Hispanic Heritage Month is celebrated in the U.S. every year from Sept. 15 through Oct. 15, commemorating the contribution made to American life by the Hispanic community.

For purposes of this celebration, the term Hispanic includes persons with ancestry from the countries of Argentina, Belize, Bolivia, Brazil, Chile, Colombia, Cuba, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Paraguay, Panama, Peru, Spain, Uruguay and Venezuela. Puerto Rico is also included in the celebration.

The term Hispanic, as defined by the U.S. Census Bureau, refers to Spanish-speaking people in the United States of any race. On the 2000 Census form, people of Spanish, Hispanic or Latino origin could identify themselves as Mexican, Puerto Rican, Cuban or "other Spanish/Hispanic/Latino". More than 35 million people identified themselves as Hispanic or Latino in that Census.

Each year the National Council of Hispanic Employment Program Managers Council and the Hispanic Foundation select a theme for the month and commission a poster to reflect that theme. This year's theme is "Keeping the Promise: Unity, Strength, Leadership." Events and activities vary widely across the country, ranging from lectures on ethnicity to cultural, musical, theatrical, social and sporting activities.

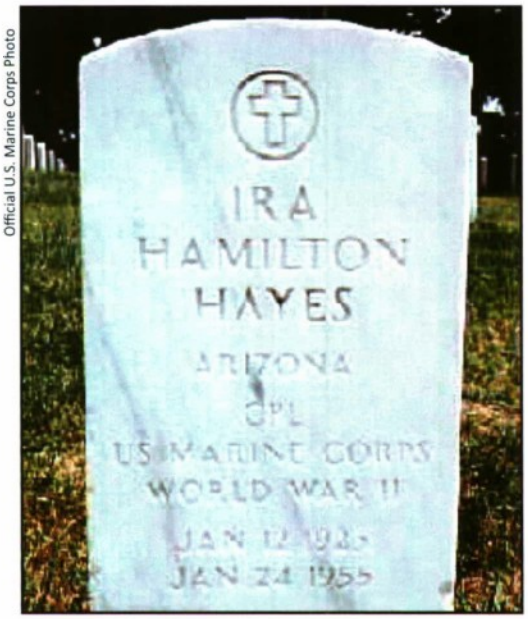
The dates of the observance coincide with the anniversary dates of the independence of seven Latin American countries: Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Mexico and Chile.

Hispanic colonists settled in Florida, Louisiana and New Mexico, and two of the oldest communities in the United States — St. Augustine, FL (1565) and Santa Fe, NM (1610) — have had Hispanic inhabitants since they were established.

The Department of Veterans Affairs (VA) notes that Hispanic Veterans are the country's largest ethnic group with more than 1.1 million Veterans. Hispanic Americans have fought in every American war.

Hispanic Americans have also enriched our country beyond measure — in science and technology, education, the arts, sports, business, government — and in our military.

Whatever their individual backgrounds' before they came to serve their country, Hispanics have found opportunities by donning the uniforms of the Army, Navy, Air Force and Marines. Some, like Joseph Medina, came from a family with a rich military background. Others, like Eva Jacques or Raymond Ayon, were students enticed with the notion that their country needed them. None expressed that even a hint of prejudice marked their experiences, a remarkable testimony to the democratic ideal of military service.



Official U.S. Marine Corps Photo

Hayes lies in Section 34 of Arlington National Cemetery (Jan. 12, 1923 – Jan. 24, 1955)

Iwo Jima Flag Raiser – Ira Hayes

From Armed Forces Press Service

Noted World War II hero and Pima Indian, Ira Hamilton Hayes, was born on the Pima Reservation, Sacaton, AZ, on Jan. 12, 1923. His parents, Joe E. and Nancy W. Hayes, were farmers.

Although Hayes had a normal childhood on the reservation, his life changed dramatically when war broke out and he joined the Marine Corps. Previous to his enlistment, Hayes had rarely been off the reservation. His chief told him to be an "Honorable Warrior" and to bring honor upon his family.

A dedicated Marine, quiet and steady, Hayes was admired by his fellow Marines who fought alongside him in three Pacific battles. After completing courses under the U.S. Marine Corps Parachutist School at San Diego, he was lovingly dubbed "Chief

Falling Cloud," and assigned to a parachute battalion of the Fleet Marine Force.

By the beginning of 1945, Hayes was part of the American invasion force that attacked the Japanese stronghold of Iwo Jima. On Feb. 23, 1945, to signal the end of Japanese control, Hayes and five others raised the U. S. flag atop Mount Suribachi on the island of Iwo Jima. Three of the six men were killed shortly after the raising the flag. This heroic act was photographed by Joe Rosenthal, and it transformed Hayes' life forever. Subsequently a U.S. postage stamp was created to commemorate the event, as well as bronze statue in Washington, DC.

President Franklin D. Roosevelt called the brave survivors of the flag raising back to the United States to aid a war bond drive.

At the White House, following Roosevelt's death, President Truman told Hayes, "You are an American hero."

But Hayes didn't feel pride. As he later lamented, "How could I feel like a hero when only five men in my platoon of 45 survived; when only 27 men in my company of 250 managed to escape death or injury?"

Later, the surviving flag raisers were shuttled from one city to another for publicity purposes. Hayes asked to be sent back to the front lines, stating that, "sometimes I wish that guy (Joe Rosenthal) had never made that picture."

The Bond Tour was an ordeal for Hayes. He couldn't understand or accept the adulation. "It was supposed to be soft duty, but I couldn't take it," Hayes said. "Everywhere we went people shoved drinks in our hands and said, 'You're a Hero!' We knew we hadn't done that much, but you couldn't tell them that."

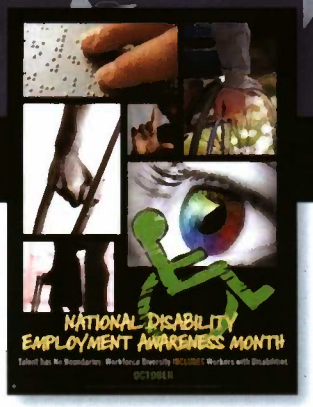
At the conclusion of World War II, Hayes went back to the reservation attempting to lead an anonymous life. But it didn't turn out that way.

"I kept getting hundreds of letters. And people would drive through the reservation, walk up to me and ask, 'Are you the Indian who raised the flag on Iwo Jima?'" said Hayes.

Hayes tried to drown his "Conflict of Honor" with alcohol. Arrested as drunk and disorderly, his pain was clear. Hayes stated, "I was sick. I guess I was about to crack up thinking about all my good buddies. They were better men than me and they're not coming back, much less back to the White House, like me."

He was never able to get his life back in balance again. Hayes died of exposure at the age of 33 on Jan. 24, 1955. He was memorialized by the Pima people and characterized as "a hero to everyone but himself." He is buried in Arlington National Cemetery.

Of the six flag raisers in the photo, the front four are (left to right) Ira Hayes, Franklin Sousley, John Bradley and Harlon Block. The back two are Michael Strank (behind Sousley) and Rene Gagnon (behind Bradley). Strank, Block and Sousley would die shortly afterwards. Bradley, Hayes and Gagnon became national heroes within weeks. (Photo by Joe Rosenthal, AP Photographer)



BIG Conference Highlights Diversity, Individual Achievements

By LT Laura K. Stegherr, Diversity Directorate Public Affairs

BOSTON -- The Navy took a central role in the 33rd annual Blacks in Government (BIG) National Training Conference in Boston, Aug. 22 - 25.

BIG was established in 1975 to bring together African-Americans in public service to confront workplace and community issues. Today, the non-profit organization's goals are to promote equity in the workplace, excellence in public service and opportunity for all Americans.

The conference brought together nearly a thousand individuals from more than 20 government agencies for four days of seminars, panels and professional development sessions.

"This year's theme, 'Explore and Navigate Your Leadership Journey Through BIG!,' encourages each of us to become leaders and to make an impact not only within our Federal, state or local government workplaces, but in our daily lives as well," said BIG National President J. David Reeves. "The world is calling for leaders of all kinds, but leadership often requires training, education and experience. Equally important is the need for us to prepare the next generation of leaders to face future challenges. This year's [conference] is designed to do these things and more."

CAPT Thomas Whittles, deputy commander, Navy Intelligence Reserve Command, provided remarks at the BIG President's Reception and explained the strategic role of diversity for the Navy, as well as the importance of organizations such as BIG.

"The Navy understands that diversity is indeed a strategic imperative that impacts our mission readiness," said Whittles. "We know that we become a stronger force as we draw from the best of America inherent in the rich diversity of our nation. As we operate globally, we must have intrinsic in our force a diversity of ideas, experiences, expertise and backgrounds to fulfill the variety of missions asked of us -- our ability to defend our nation and to serve with excellence as America's Global Force for Good depends on it.

"As we move forward, our strong partnerships with organizations such as BIG are so important," said Whittles. "We must work together to inspire and mentor the youth of America -- encouraging them to consider serving their country as a Sailor or civilian in the United States Navy."

> ***" We must work together to inspire and mentor the youth of America -- encouraging them to consider serving their country as a Sailor or civilian in the United States Navy."***
>
> ***Deputy* Commander, Navy Intelligence Reserve Command**
> **CAPT Thomas Whittles**

The conference featured a Department of Defense forum during which DoD employees had the opportunity to hear presentations from several senior DoD leaders including John H. James, Jr., executive director of Missile Defense Agency, and Paige Hinkle Bowles, principal director of Civilian Personnel Policy.

The DoD forum featured an awards ceremony honoring military members and DoD civilian employees who demonstrated role model qualities and the core values of the military service. CDR George Floyd, assistant reactor officer aboard USS Nimitz (CVN 68), and Kevin Hines, a technical specialist at Naval Undersea Warfare Center Keyport, WA, both received BIG's Meritorious Service Award.

Floyd was recognized for his career-long efforts to build bridges for current and future generations of African-American servicemen and women, through campus recruiting visits to Historically Black Colleges and Universities (HBCUs), organization of a school adoption program for disadvantaged Hispanic and African American youth, and participation in the National Naval Officers Association, the sea services' organization for mentoring and professional development of African American Sailors, officers and civilians.

Additionally, Floyd was named the Black Engineer of the Year's "Most Promising Engineer" in 2009, and in 2010 he received its Roy Wilkins Award for Leadership by the National Association for Advancement of Colored People.

Hines was honored for his efforts establishing a relationship with students in the business and engineering programs at Prairie View A&M University in Texas, an HBCU, assisting in recruitment of the students and offering mentorship to new hires. He helped recruit students to Keyport and once they were hired, offered them one-on-one mentorship. Of the 60 Prairie View students interviewed, Keyport

hired nine who are now employed as logistics management specialists, electrical engineers and mechanical engineers.

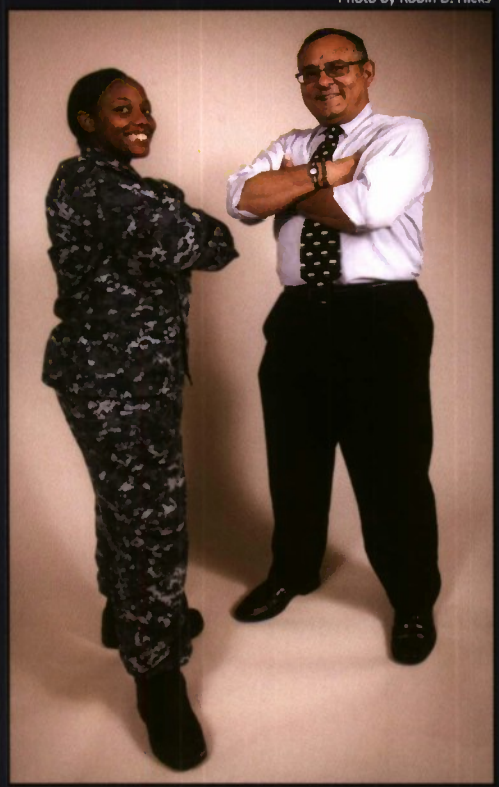
The Navy partnered with BIG in facilitating their Future Leaders in America's Government program, which brought nearly 50 junior and senior high school students to the conference Aug. 24 for several informational sessions, including seminars on ways to pay for college, healthy lifestyle and personal finances.

The Navy's participation in the BIG conference is part of a national outreach initiative to engage and connect with youth, educational, civic, government and business leaders across the country, and to communicate the importance of educating and training future leaders from diverse segments of society in the areas of Science, Technology, Engineering and Mathematics.

For more news from Chief of Naval Personnel - Diversity Directorate, visit www.navy.mil/local/cnp-diversity/.

DIVERSITY SPOTLIGHT

Photo by Robin D. Hicks



(Left) YN1(SW) Classie Mejia works in CYBERFOR's Reserve Manpower Division as the Deputy Operational Support Officer. She has been involved in the Diversity program since March 2011. She is responsible for ensuring the command is informed of the many diversity awards that are available.

(Right) George Bieber is CYBERFOR's Deputy Public Affairs Officer and editor of the command's quarterly publication InfoDOMAIN. He has edited, designed and published Diversity articles, pictures and events since the program's inception in 2007. He continues to highlight special months, days and CYBERFOR's Sailors and civilians' involvement in the Navy-wide program.

UPCOMING DIVERSITY CONFERENCES

CONFERENCE	LOCATION	DATES	WEBSITE
Japanese American Citizens League (JACL) National Gala	Washington, DC	29 September	www.jacl.org
The Society of Mexican American Engineers and Scientists, Inc., (MAES) Symposium	Oakland, CA	5-8 October	www.maes-natl.org
Hispanic Engineer National Achievements Awards Corporation (HENAAC) Conference	Orlando, FL	6-8 October	www.greatmindsinstem.org
Society of Women Engineers (SWE) Conference	Chicago	13-15 October	www.swe.org
The Thurgood Marshall College Fund (TMCF) Leadership Training Institute Recruitment Conference and Career Fair	New York	21-24 October	www.thurgoodmarshallfund.org
Society of Hispanic Professional Engineers (SHPE)	Anaheim, CA	26-30 October	www.shpe.org
11th Edition of the African American Yearbook Reception	Washington, DC	TBD October	www.africanamericanyearbook.com/index.php
MANA Las Primas Gala	Washington, DC	TBD October	www.hermana.org
National Women of Color (NWOC) in Technology Conference	Dallas, TX	3-5 November	www.womenofcolor.net
Grace Hopper Celebration of Women in Computing	TBD	8-12 November	www.gracehopper.org
American Indian Science and Engineering Society (AISES) Conference	Minneapolis, MN	10-12 November	www.aises.org

FOR MORE INFORMATION ON CYBERFOR'S DIVERSITY PROGRAM CONTACT: LCOR CHRISTINE COCHRAN AT (757) 492-8827 X 2 OR CHRISTINE.COCHRAN@NAVY.MIL

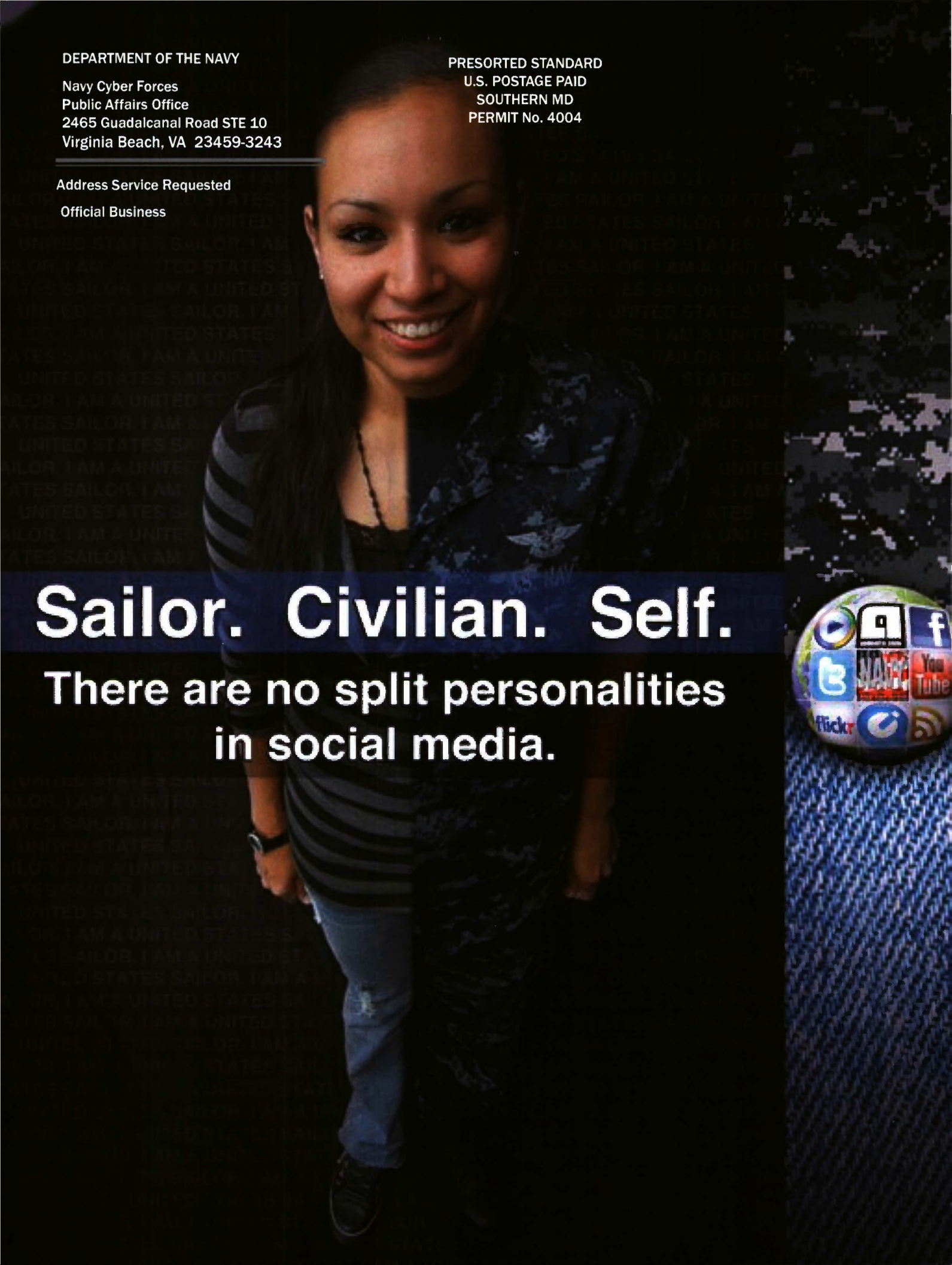
DEPARTMENT OF THE NAVY

Navy Cyber Forces
Public Affairs Office
2465 Guadalcanal Road STE 10
Virginia Beach, VA 23459-3243

PRESORTED STANDARD
U.S. POSTAGE PAID
SOUTHERN MD
PERMIT No. 4004

Address Service Requested

Official Business



Sailor. Civilian. Self.

There are no split personalities in social media.